

Capítulo 3

El anillo de polinomios sobre un cuerpo

3.1. Generalidades sobre polinomios

Definición 37. Sea A un anillo conmutativo, y x un elemento que no pertenece a A . Un polinomio con coeficientes en A es una expresión de la forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde $n \in \mathbb{N}$ y $a_k \in A$.

Nota: Recordemos que un anillo conmutativo es un conjunto A en el que hay definidas dos operaciones, $+$ y \cdot (suma y producto), que son asociativas, conmutativas y tienen elemento neutro (0 para la suma y 1 para el producto), todo elemento tiene un inverso (opuesto) para la suma, y la suma es distributiva respecto al producto.

Básicamente, un anillo es un conjunto en el que podemos sumar, restar y multiplicar los elementos, con las propiedades usuales de estas operaciones.

Ejemplos de anillos que utilizaremos son \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} y \mathbb{Z}_n .

Ejemplo 3.1.1. Son polinomios con coeficientes en \mathbb{Z}

$$2x^2 + 3x + (-1); \quad 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2$$

En el primer caso $n = 2$, $a_2 = 2$, $a_1 = 3$ y $a_0 = -1$, mientras que en el segundo $n = 5$ y $a_5 = a_4 = a_3 = a_2 = a_1 = a_0 = 2$.

No son polinomios con coeficientes en \mathbb{Z}

$$3x^2 - x + 2 + x^{-1}; \quad \sin(x) - 3$$

Nota: La definición que se ha dado no es muy rigurosa. De hecho, con esa definición, la expresión $x^2 + 1$ no es un polinomio, pues no se ajusta a lo explicitado en dicha definición, ya que no está dicho quien es a_1 ni a_2 . Si es un polinomio, de acuerdo con la definición dada $1x^2 + 0x + 1$. Obviamente, al referirnos al polinomio $1x^2 + 0x + 1$ lo haremos como $x^2 + 1$. De la misma forma, el primer polinomio que aparece en el ejemplo anterior lo escribiremos $2x^2 + 3x - 1$.

En general, si $a_k x^k + \cdots + a_1 x + a_0$ es un polinomio y $a_i = 0$, entonces el polinomio dado diremos que es igual a $a_k x^k + \cdots + a_{i+1} x^{i+1} + a_{i-1} x^{i-1} + \cdots + a_0$ (salvo que el polinomio de partida sea 0).

Tampoco se ajusta a la definición que hemos dado de polinomio, por ejemplo, la expresión $5 + 2x + 3x^2$. Deberíamos escribir $3x^2 + 2x + 5$.

En lo que sigue no tendremos en cuenta estas deficiencias de la definición dada.

Dado un anillo A denotaremos por $A[x]$ al conjunto de todos los polinomios con coeficientes en A .

Definición 38. Sea A un anillo.

1. Sean $p(x) = a_mx^m + \cdots + a_1x + a_0$ y $q(x) = b_nx^n + \cdots + b_1x + b_0$ dos elementos de $A[x]$, y supongamos que $m \leq n$. Se define la suma de los polinomios $p(x)$ y $q(x)$ como el polinomio

$$p(x) + q(x) = b_nx^n + \cdots + b_{m+1}x_{m+1} + (a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

2. Sea $k \in \mathbb{N}$, $p(x) = a_mx^m + \cdots + a_1x + a_0$, $q(x) = b_kx^k \in A[x]$ (si $k = 0$ entonces $q(x) = b_0$). Se define el producto de $p(x)$ y $q(x)$ como el polinomio:

$$p(x) \cdot q(x) = a_nb_kx^{k+n} + \cdots + a_1b_kx^{k+1} + a_0b_kx^k$$

Sean ahora $p(x) = a_mx^m + \cdots + a_1x + a_0$ y $q(x) = b_nx^n + \cdots + b_1x + b_0$. Se define el producto de $p(x)$ y $q(x)$ como

$$p(x) \cdot q(x) = p(x) \cdot q_n(x) + \cdots + p(x) \cdot q_1(x) + p(x) \cdot q_0(x)$$

donde $q_k(x) = b_kx^k$.

Las dos operaciones definidas satisfacen las siguientes propiedades:

- ▮ La suma de polinomios es asociativa, es decir, $p(x) + (q(x) + r(x)) = (p(x) + q(x)) + r(x)$. Nótese que esta propiedad es necesaria para poder definir el producto tal y como se ha hecho aquí.
- ▮ La suma de polinomios es conmutativa.
- ▮ La suma tiene un elemento neutro. Éste será denotado por 0.
- ▮ Dado $p(x) \in A[x]$ existe $q(x) \in A[x]$ tal que $p(x) + q(x) = 0$. Denotaremos como $-p(x)$ a este polinomio.
- ▮ El producto de polinomios es asociativo y conmutativo.
- ▮ El producto tiene un elemento neutro. Éste será denotado por 1.
- ▮ La suma es distributiva con respecto al producto.

Estas propiedades nos dicen que, si A es un anillo conmutativo, entonces $A[x]$ es también un anillo conmutativo.

Además, podemos identificar A como los elementos de $A[x]$ de la forma $p(x) = a$, en cuyo caso A es un subanillo de $A[x]$.

Ejemplo 3.1.2. Sea $A = \mathbb{Z}_{12}$, y sean $p(x) = 2x^3 + 3x^2 + 7x + 9$ y $q(x) = 6x^2 + 5x + 4$. Entonces:

$$\begin{aligned} * \quad p(x) + q(x) &= 2x^3 + (3+6)x^2 + (7+5)x + (9+4) = 2x^3 + 9x^2 + 1 \\ * \quad p(x) \cdot q(x) &= p(x) \cdot (6x^2) + p(x) \cdot (5x) + p(x) \cdot 4 \\ &= (0x^5 + 6x^4 + 6x^3 + 6x^2) + (10x^4 + 3x^3 + 11x^2 + 9x) + (8x^3 + 0x^2 + 4x + 0) \\ &= 4x^4 + 5x^3 + 5x^2 + x \end{aligned}$$

Normalmente, para efectuar la multiplicación dispondremos los datos de la siguiente forma:

$p(x)$	2	3	7	9	
$q(x)$		6	5	4	
$p(x) \cdot 4$		8	0	4	0
$p(x) \cdot 5x$	10	3	11	9	
$p(x) \cdot 6x^2$	0	6	6	6	
$p(x) \cdot q(x)$	0	4	5	5	1

luego el resultado final es $4x^4 + 5x^3 + 5x^2 + x$.

Daremos a continuación algunos conceptos referentes a los polinomios:

Definición 39. Sea A un anillo conmutativo y $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x]$.

- i) Si $a_n \neq 0$ entonces se dice que el polinomio $p(x)$ tiene **grado n** ($gr(p(x)) = n$). Nótese que no se ha definido el grado del polinomio 0. En ocasiones, consideraremos que el grado del polinomio 0 es -1 .
- ii) Al elemento $a_k \in A$ se le llama **coeficiente de grado k** , y a la expresión $a_k x^k$, **término de grado k** .
- iii) El coeficiente de grado n de un polinomio de grado n se llama **coeficiente líder**, y a la expresión $a_n x^n$ **término líder**.
- iv) El coeficiente de grado 0 de un polinomio se le llama **término independiente**.
- v) Un polinomio cuyo coeficiente líder valga 1 se dice que es un **polinomio mónico**.
- vi) Un polinomio que, bien tiene grado 0, o bien es el polinomio 0 se dice que es un **polinomio constante**.

Ejemplo 3.1.3. Sean $p(x) = 3x^3 + 5x + 2$ y $q(x) = x^4 + 2x^3 + 3x^2 + 5x + 8$ dos polinomios con coeficientes en \mathbb{Z}_{11} . Entonces:

- $gr(p(x)) = 3$ y $gr(q(x)) = 4$.
- El coeficiente de grado 2 de $p(x)$ es 0, mientras que el coeficiente de grado 2 de $q(x)$ es 3. El coeficiente de grado 5 de $q(x)$ es cero.
- El coeficiente líder de $p(x)$ es 3, mientras que el coeficiente líder de $q(x)$ es 1. Por tanto, $q(x)$ es mónico, mientras que $p(x)$ no lo es.
- Los términos independientes de $p(x)$ y $q(x)$ son 2 y 8 respectivamente.
- Ninguno de los dos polinomios son constantes.

Proposición 3.1.1. Sean $p(x), q(x) \in A[x]$. Entonces:

$$gr(p(x) + q(x)) \leq \max\{gr(p(x), q(x))\}$$

$$gr(p(x) \cdot q(x)) \leq gr(p(x)) + gr(q(x))$$

La demostración de ambos hechos es fácil. Podría pensarse que en el segundo caso se da siempre la igualdad ($gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$). Sin embargo, el Ejemplo 3.1.2 nos muestra un caso en el que se da la desigualdad estricta.

Es fácil comprobar que si $p(x)$ o $q(x)$ es mónico, entonces se verifica que $gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$.

Terminamos esta sección estudiando la evaluación de un polinomio en un punto.

Definición 40. Sea A un anillo, $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$ y $a \in A$. Se define la evaluación de $p(x)$ en el punto a , $Ev_a(p(x))$ como el elemento de A :

$$Ev_a(p(x)) = a_n a^n + \cdots + a_1 a + a_0$$

Dicho de otra forma, $Ev_a(p(x))$ es el resultado de sustituir en la expresión de $p(x)$ el símbolo x por a . De esta forma tenemos definida una aplicación (morfismo de anillos) $Ev_a : A[x] \rightarrow A$.

Normalmente, escribiremos $p(a)$ en lugar de $Ev_a(p(x))$.

Proposición 3.1.2. Dado A un anillo y $p_1(x), p_2(x) \in A[x]$

1. Si $q(x) = p_1(x) + p_2(x)$ entonces $q(a) = p_1(a) + p_2(a)$ (es decir, $Ev_a(p_1(x) + p_2(x)) = Ev_a(p_1(x)) + Ev_a(p_2(x))$).
2. Si $q(x) = p_1(x) \cdot p_2(x)$ entonces $q(a) = p_1(a) \cdot p_2(a)$ (es decir, $Ev_a(p_1(x) \cdot p_2(x)) = Ev_a(p_1(x)) \cdot Ev_a(p_2(x))$).

Usando la aplicación evaluación, cada polinomio de $A[x]$ determina una aplicación $A \rightarrow A$, dada por $a \mapsto p(a)$.

Ejemplo 3.1.4.

1. El polinomio $x^3 + 3x^2 + 2x + 2 \in \mathbb{Z}_5[x]$ determina la aplicación $\mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ siguiente:

$$0 \mapsto 2 \quad 1 \mapsto 3 \quad 2 \mapsto 1 \quad 3 \mapsto 2 \quad 4 \mapsto 2$$

2. El polinomio $x^2 + x + 1 \in \mathbb{Z}_2[x]$ determina la aplicación

$$0 \mapsto 1 \quad 1 \mapsto 1$$

es decir, la aplicación constante 1.

3.2. Máximo común divisor y mínimo común múltiplo

Definición 41. Sean $p(x), q(x) \in A[x]$. Se dice que $p(x)$ divide a $q(x)$, o que $q(x)$ es múltiplo de $p(x)$, y escribiremos $p(x)|q(x)$, si existe $c(x) \in A[x]$ verificando que $q(x) = p(x) \cdot c(x)$.

Ejemplo 3.2.1.

1. Sean $p(x) = x^2 - 1$ y $q(x) = 2x + 2$ dos polinomios con coeficientes en \mathbb{Q} . Entonces $q(x)|p(x)$, pues $p(x) = q(x) \cdot (\frac{1}{2}x - \frac{1}{2})$. Sin embargo, si consideramos ambos polinomios en $\mathbb{Z}[x]$ entonces $q(x)$ no divide a $p(x)$.
2. En $\mathbb{Z}_2[x]$ se verifica que $(x+1)|(x^2+1)$, ya que $x^2+1 = (x+1)(x+1)$.
3. En $\mathbb{Z}_3[x]$ se verifica que $(x+1) \nmid (x^2+1)$, pues si $x^2+1 = (x+1) \cdot c(x)$, entonces $\text{gr}(c(x)) = 1$, luego $c(x) = c_1x + c_0$. Operando resulta que $c_0 = 1$, $c_0 + c_1 = 0$ y $c_1 = 1$, lo cual es imposible.
4. En $\mathbb{Z}_4[x]$ se verifica que $(x+2)|(2x^2+x+2)$, pues $2x^2+x+2 = (x+2)(2x+1)$ y $(2x^2+x+2)|(x+2)$ pues $x+2 = (2x^2+x+2)(2x+1)$.
5. Para cualquier $p(x) \in A[x]$ se verifica que $1|p(x)$ y $p(x)|0$.

En lo que sigue nos centraremos en polinomios con coeficientes en un cuerpo, o con coeficientes en \mathbb{Z} . Recordemos que un cuerpo es un anillo conmutativo en el que cada elemento no nulo tiene un inverso para el producto. Dicho de otra forma, es un conjunto en el que podemos sumar, restar, multiplicar y dividir (salvo por 0). Ejemplos de cuerpos son \mathbb{Q} , \mathbb{R} , \mathbb{C} o \mathbb{Z}_p , donde p es un número primo.

Veamos a continuación algunas propiedades referentes a la relación de divisibilidad de polinomios.

Proposición 3.2.1. Sea K un cuerpo y $p(x), q(x), r(x) \in K[x]$. Entonces:

1. $p(x)|p(x)$.
2. Si $p(x)|q(x)$ y $q(x)|p(x)$, entonces existe $a \in K^*$ tal que $q(x) = a \cdot p(x)$.
3. Si $p(x)|q(x)$ y $q(x)|r(x)$, entonces $p(x)|r(x)$.
4. Si $p(x)|q(x)$ y $p(x)|r(x)$, entonces $p(x)|(q(x) + r(x))$.
5. Si $p(x)|q(x)$, entonces $p(x)|q(x) \cdot r(x)$ para cualquier $r(x) \in K[x]$.

La demostración de estas propiedades es casi inmediata.

Si trabajamos con polinomios con coeficientes en \mathbb{Z} , todas las propiedades son iguales salvo la segunda. Se pide estudiar que ocurre si tenemos dos polinomios $p(x), q(x) \in \mathbb{Z}[x]$ tales que $p(x)|q(x)$ y $q(x)|p(x)$.

Los apartados 1,3,4,5 son igualmente válidos para polinomios con coeficientes en un anillo conmutativo A . El ejemplo 3.2.1.4 nos dice que el apartado 2 no es válido en general.

Antes de estudiar el máximo común divisor y el mínimo común múltiplo de dos polinomios veamos cómo dividir polinomios.

Teorema 3.2.1 (Algoritmo de la división). *Sea K un cuerpo, y $p(x), q(x)$ dos polinomios de $K[x]$, con $q(x) \neq 0$. Entonces existen únicos polinomios $c(x), r(x) \in K[x]$ tales que:*

$$p(x) = q(x) \cdot c(x) + r(x)$$

$$r(x) = 0 \text{ o } gr(r(x)) < gr(q(x)).$$

Los polinomios $c(x)$ y $r(x)$ son llamados cociente y resto respectivamente.

Demostración:

Vamos a dar una indicación de como sería la demostración de existencia.

Supongamos que $gr(q(x)) = m$ y que b_m es el coeficiente líder de $q(x)$.

Distingamos dos casos:

- ▮ $gr(p(x)) < m$. En tal caso, basta tomar $c(x) = 0$ y $r(x) = p(x)$.
- ▮ $gr(p(x)) \geq m$. Llamemos entonces n al grado de $p(x)$ y sea a_n su coeficiente líder. Sea entonces $c_1(x) = a_n \cdot (b_m)^{-1} x^{n-m}$ y $p_1(x) = p(x) - q(x) \cdot c_1(x)$. Se tiene entonces que:
 - $p(x) = q(x) \cdot c_1(x) + p_1(x)$. Esto es evidente por cómo hemos definido $p_1(x)$.
 - $gr(p_1(x)) < gr(p(x))$ o $p_1(x) = 0$. Esto es así porque el término líder de $q(x) \cdot c_1(x)$ vale $-a_n x^n$. Por tanto, al hacer la resta $p(x) - q(x) \cdot c_1(x)$, el coeficiente líder de $p(x)$ se anula con el coeficiente líder de $q(x) \cdot c_1(x)$.

Si ahora $gr(p_1(x)) < m$ (o $p_1(x) = 0$), ya hemos terminado. Basta tomar $c(x) = c_1(x)$ y $r(x) = p_1(x)$. En caso contrario, repetimos con $p_1(x)$ el mismo proceso que con $p(x)$.

Obtenemos así dos polinomios $p_2(x)$ y $c_2(x)$ tales que $p_1(x) = q(x) \cdot c_2(x) + p_2(x)$ y $gr(p_2(x)) < gr(p_1(x))$ o $p_2(x) = 0$. En tal caso, se tiene que:

$$p(x) = q(x) \cdot c_1(x) + p_1(x) = q(x) \cdot c_1(x) + q(x) \cdot c_2(x) + p_2(x) = q(x) \cdot (c_1(x) + c_2(x)) + p_2(x)$$

Obtenemos así dos sucesiones de polinomios $c_1(x), c_2(x), \dots, c_k(x)$ y $p_1(x), p_2(x), \dots, p_k(x)$ satisfaciendo

$$▮ \quad p(x) = q(x) \cdot (c_1(x) + c_2(x) + \dots + c_k(x)) + p_k(x)$$

$$▮ \quad p_k(x) = 0 \text{ ó } gr(p_k(x)) < gr(p_{k-1}(x)) < \dots < gr(p_1(x)) < gr(p(x)).$$

Este proceso lo continuamos hasta que $gr(p_k(x))$ sea menor que m o $p_k(x)$ sea igual al polinomio cero. En tal caso, basta tomar $c(x) = c_1(x) + \dots + c_k(x)$ y $r(x) = p_k(x)$.

La demostración de la unicidad se deja como ejercicio.

■

Nótese que si en lugar de considerar un cuerpo consideramos un anillo conmutativo cualquiera, y $p(x), q(x)$ son dos polinomios tales que el coeficiente líder de $q(x)$ es una unidad, entonces podría repetirse la demostración.

Por tanto, si $p(x), q(x) \in A[x]$ y $q(x)$ es mónico, existe únicos $c(x), r(x) \in A[x]$ tales que $p(x) = q(x) \cdot c(x) + r(x)$, y $gr(r(x)) < gr(q(x))$ o $r(x) = 0$.

Ejemplo 3.2.2. *Calculemos el cociente y el resto de la división del polinomio $p(x) = 2x^4 + 3x^3 + 5x + 1$ entre $q(x) = 3x^3 + x + 6$ en $\mathbb{Z}_7[x]$. Lo haremos siguiendo los pasos hechos en la demostración precedente.*

Notemos en primer lugar que $gr(p(x)) > gr(q(x))$.

Calculamos 3^{-1} . Se tiene que $3^{-1} = 5$.

Tomamos entonces el polinomio $c_1(x) = 2 \cdot 5 \cdot x^{4-3} = 3x$.

Hallamos $p_1(x) = p(x) - 3xq(x) = p(x) + 4xq(x) = 3x^3 + 4x^2 + x + 1$.

Dado que $gr(p_1(x)) \geq gr(q(x))$ continuamos dividiendo. Tomamos el polinomio $c_2(x) = 3 \cdot 5x^{3-3} = 1$

Hallamos $p_2(x) = p_1(x) - 1q(x) = p_1(x) + 6q(x) = 4x^2 + 2$.

Dado que $gr(p_2(x)) < gr(q(x))$ la división ha terminado. El cociente es $c(x) = c_1(x) + c_2(x) = 3x + 1$ y el resto $r(x) = 4x^2 + 2$.

Los cálculos podemos disponerlos como sigue:

$$\begin{array}{r}
 \begin{array}{cccc|cccc}
 2 & 3 & 0 & 5 & 1 & 3 & 0 & 1 & 6 \\
 5 & 0 & 4 & 3 & & 3 & 1 & & \\
 \hline
 3 & 4 & 1 & 1 & & & & & \\
 4 & 0 & 6 & 1 & & & & & \\
 \hline
 4 & 0 & 2 & & & & & &
 \end{array}
 \end{array}$$

Si analizamos el estudio que hicimos de los números enteros, podemos ver como el algoritmo de la división resultó clave en el desarrollo posterior. A partir de él se pudo probar la existencia de máximo común divisor y calcularlo; encontrar los coeficientes de Bezout, que luego fueron la base para la resolución de congruencias.

Ahora, en $K[x]$ tenemos también un algoritmo de división, luego todo lo dicho para números enteros vale también para polinomios. En lo que sigue, trasladaremos los resultados del tema anterior al caso de los polinomios, incidiendo en las particularidades de éstos.

Nota: Un anillo A , se dice que es un dominio euclídeo si en él tenemos definida una aplicación *grado*, $g : A^* \rightarrow \mathbb{N}$ satisfaciendo dos propiedades:

- ▮ $g(ab) \geq g(a)$ para $b \neq 0$
- ▮ Para todo $a, b \in A$, $b \neq 0$, existen $q, r \in A$ tales que $a = bq + r$ y $g(r) < g(a)$ o $r = 0$.

Es decir, un Dominio Euclídeo viene a ser un anillo en el que tenemos definida una división, con resto.

Tenemos entonces que \mathbb{Z} y $K[x]$ son dominios euclídeos (las funciones grado son, en el caso de \mathbb{Z} el valor absoluto, y en el caso de $K[x]$ el grado).

En un dominio euclídeo se verifica el teorema de Bezout, el teorema chino del resto, el teorema de factorización única, etc.

Definición 42. Sean $p(x), q(x) \in K[x]$, con $q(x) \neq 0$. Se definen los polinomios $p(x)$ mód $q(x)$ y $p(x)$ div $q(x)$ como el resto y el cociente de dividir $p(x)$ entre $q(x)$.

Cuando $p(x)$ mód $q(x) = 0$, denotaremos por $\frac{p(x)}{q(x)}$ al polinomio $p(x)$ div $q(x)$.

Ejemplo 3.2.3.

1. En $\mathbb{Z}_3[x]$, se verifica que:

$$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ mód } x^2 + 2x + 1 = 2$$

$$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ div } x^2 + 2x + 1 = x^3 + 2x^2 + 2.$$

2. En $\mathbb{Z}_5[x]$:

$$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ mód } x^2 + 2x + 1 = 6x$$

$$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ div } x^2 + 2x + 1 = x^3 + 4x^2 + 3x + 1.$$

Definición 43. Sea $p(x) \in A[x]$ y $a \in A$. Se dice que a es una raíz de $p(x)$ si $p(a) = 0$.

Ejemplo 3.2.4. El polinomio $p(x) = x^5 + x^4 + x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$ tiene a $x = 1$ por raíz, pues $p(1) = 1 + 1 + 1 + 2 + 1 = 0$. Sin embargo, 0 no es raíz pues $p(0) = 1$ y 2 tampoco es raíz pues $p(2) = 2^5 + 2^4 + 2^3 + 2 \cdot 2^2 + 1 = 2 + 1 + 2 + 2 + 1 = 2$.

El siguiente resultado es un conocido teorema referente a la división por el polinomio $x - a$.

Teorema 3.2.2 (Teorema del resto). Sea $p(x) \in A[x]$ y $a \in A$. Entonces el resto de dividir $p(x)$ entre $x - a$ es el resultado de evaluar $p(x)$ en el punto a . Dicho de otra forma

$$p(x) \bmod x - a = p(a)$$

Demostración: Si dividimos $p(x)$ entre $x - a$ nos da un polinomio de grado menor que 1, luego debe ser un polinomio constante. Se tiene entonces que $p(x) = c(x) \cdot (x - a) + r$. Evaluando en a nos queda que $p(a) = c(a) \cdot (a - a) + r$, es decir, $r = p(a)$. ■

Corolario 3.2.1 (Teorema del factor). Sea $p(x) \in A[x]$ y $a \in A$. Entonces a es raíz de $p(x)$ si, y sólo si, $(x - a) | p(x)$.

En la siguiente proposición veremos una forma rápida de calcular el cociente y el resto de la división de un polinomio entre $x - a$.

Proposición 3.2.2. Sea $p(x) \in A[x]$, $a \in A$. Supongamos que $p(x) = a_n x^n + \cdots + a_1 x + a_0$ y que $p(x) = (b_{n-1} x^{n-1} + \cdots + b_1 x + b_0)(x - a) + r$. Entonces:

$$b_{n-1} = a_n$$

$$b_{i-1} = a_i + b_i a \text{ para } i = 0, 1, \dots, n-1$$

$$r = a_0 + b_0 a$$

La demostración se deja como ejercicio.

Esta proposición proporciona el conocido método de Ruffini (algoritmo de Horner) para dividir un polinomio entre $x - a$.

Para esto se disponen los datos conocidos como sigue:

$$\begin{array}{c|cccccccc} a & a_n & a_{n-1} & \cdots & a_{i+1} & a_i & \cdots & a_1 & a_0 \\ \hline & b_{n-1} & b_{n-2} & \cdots & b_i & b_{i-1} & \cdots & b_0 & r \end{array}$$

Para calcular los coeficientes b_i se procede como sigue:

Se comienza por $b_{n-1} = a_n$

Supuesto calculado b_i se calcula b_{i-1} como $b_{i-1} = a_i + b_i a$.

Por último, hallado b_0 se calcula r como $r = a_0 + b_0 a$.

Para ordenar los cálculos se coloca el valor $b_i a$ justo debajo del valor de a_i , y se efectúa la suma, obteniéndose así el valor de b_{i-1} .

$$\begin{array}{c|cccccccc} a & a_n & a_{n-1} & \cdots & a_{i+1} & a_i & \cdots & a_1 & a_0 \\ & & & & & b_i a & & & \\ \hline & b_{n-1} = a_n & b_{n-2} & \cdots & b_i & b_{i-1} = a_i + b_i a & \cdots & b_0 & r \end{array}$$

Ejemplo 3.2.5. Vamos a hallar el cociente y el resto de la división de $x^5 + x^4 + x^3 + 2x^2 + 1$ entre $x - 2$ en $\mathbb{Q}[x]$. Para ello procedemos a completar la tabla

	1	1	1	2	0	1
2						

Rellenando de izquierda a derecha.

	1	1	1	2	0	1
2	$2 = 1 \cdot 2$	$6 = 3 \cdot 2$	$14 = 7 \cdot 2$	$32 = 16 \cdot 2$	$64 = 32 \cdot 2$	
	1	$3 = 1 + 2$	$7 = 1 + 6$	$16 = 2 + 14$	$32 = 0 + 32$	$65 = 1 + 64$

La tabla quedaría así

	1	1	1	2	0	1
2	2	6	14	32	64	
	1	3	7	16	32	65

Nótese que $x^5 + x^4 + x^3 + 2x^2 + 1 = (x^4 + 3x^3 + 7x^2 + 16x + 32)(x - 2) + 65$, y que $p(2) = 65$.

Vamos a dividir ahora $x^5 + x^4 + x^3 + 2x^2 + 1$ entre $x + 1$ en $\mathbb{Z}_3[x]$. Puesto que $x + 1 = x - 2$, se tiene que

	1	1	1	2	0	1
2	2	0	2	2	1	
	1	0	1	1	2	2

es decir, el cociente es $x^4 + x^2 + x + 2$ y el resto es 2.

Definición 44. Sea $p(x) \in A[x]$, y $a \in A$. Se dice que a es una raíz de multiplicidad m si $(x - a)^m | p(x)$ y $(x - a)^{m+1} \nmid p(x)$.

Nótese que decir que a es una raíz de multiplicidad m es decir que $p(x) = (x - a)^m c(x)$ con $c(a) \neq 0$.

A las raíces de multiplicidad 1 se les llama raíces simples; a las de multiplicidad 2, raíces dobles, a las de multiplicidad 3, raíces triples, y así sucesivamente.

En ocasiones, si a no es una raíz se dice que es una raíz de multiplicidad 0.

Ejemplo 3.2.6. El polinomio $x^5 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ tiene a $x = 1$ como raíz triple, pues $x^5 + x^3 + x^2 + 1 = (x + 1)^3(x^2 + x + 1)$, y $x^2 + x + 1$ no tiene a 1 como raíz.

	1	0	1	1	0	1
1	1	1	0	1	1	0
	1	1	0	0	1	
1	1	0	0	1	0	
	1	1	1	1		
1	1	1	1	0		
	1	1	0			
1	1	0	1			

Aquí vemos las sucesivas divisiones por $x + 1$. Se aprecia como las tres primeras son exactas, mientras que la cuarta da resto 1.

Definición 45. Sea K un cuerpo, y $p(x), q(x) \in K[x]$. Se dice que $d(x) \in K[x]$ es un máximo común divisor de $p(x)$ y $q(x)$ si:

1. $d(x)|p(x)$ y $d(x)|q(x)$.
2. Si $c(x)|p(x)$ y $c(x)|q(x)$ entonces $c(x)|d(x)$.

Nota:

1. La primera condición de la definición nos dice que $d(x)$ debe ser un divisor común de $p(x)$ y $q(x)$. La segunda condición nos dice que este divisor común es el "más grande" de los divisores comunes.
2. Si $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$ y $a \in K^*$ entonces $a \cdot d(x)$ es también un máximo común divisor de $p(x)$ y $q(x)$. De hecho, cualquier polinomio que sea un máximo común divisor de $p(x)$ y $q(x)$ es de la forma $a \cdot d(x)$. De todos estos, hay uno, y sólo uno que es mónico (salvo en el caso de que $p(x) = q(x) = 0$). Denotaremos por $\text{mcd}(p(x), q(x))$ al único máximo común divisor de $p(x)$ y $q(x)$ que es mónico.
3. La definición anterior podría haberse hecho tomando coeficientes en un anillo. En el caso de $A = \mathbb{Z}$, si $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$, también lo es $-d(x)$, y no hay más. Denotaremos por $\text{mcd}(p(x), q(x))$ al que tenga coeficiente líder positivo.
4. Aquí se ha definido el máximo común divisor de dos polinomios. Podría haberse definido de forma análoga el máximo común divisor de 3 ó más.

Se deja como ejercicio dar la definición de mínimo común múltiplo.

Veremos a continuación algunas propiedades referentes al máximo común divisor. Supongamos que tenemos $p(x), q(x), r(x), d(x) \in K[x]$, y supondremos que los cuatro polinomios son mónicos.

Propiedades:

1. $\text{mcd}(p(x), q(x)) = \text{mcd}(a \cdot p(x), q(x)) = \text{mcd}(p(x), a \cdot q(x))$, donde $a \in K^*$.
2. $\text{mcd}(p(x), 0) = p(x)$ y $\text{mcd}(p(x), 1) = 1$
3. Si $p(x)|q(x)$ entonces $\text{mcd}(p(x), q(x)) = p(x)$.
4. $\text{mcd}(p(x), \text{mcd}(q(x), r(x))) = \text{mcd}(\text{mcd}(p(x), q(x)), r(x)) = \text{mcd}(p(x), q(x), r(x))$.
5. $\text{mcd}(p(x) \cdot r(x), q(x) \cdot r(x)) = \text{mcd}(p(x), q(x)) \cdot r(x)$
6. Si $d(x)|p(x)$ y $d(x)|q(x)$ entonces $\text{mcd}\left(\frac{p(x)}{d(x)}, \frac{q(x)}{d(x)}\right) = \frac{\text{mcd}(p(x), q(x))}{d(x)}$.

Como ejercicio, se deja enunciar propiedades análogas para el mínimo común múltiplo, así como para polinomios en $\mathbb{Z}[x]$.

Los siguientes resultados son análogos a los dados para números enteros.

Lema 3.2.1. Sean $p(x), q(x) \in K[x]$. Entonces, para cualquier $c(x) \in K[x]$ se tiene que $\text{mcd}(p(x), q(x)) = \text{mcd}(q(x), p(x) - c(x)q(x))$.

Corolario 3.2.2. Sean $p(x), q(x) \in K[x]$, con $q(x) \neq 0$. Entonces $\text{mcd}(p(x), q(x)) = \text{mcd}(q(x), p(x) \bmod q(x))$.

Para calcular ahora el máximo común divisor de dos polinomios procedemos de igual forma que a la hora de calcular el máximo común divisor de dos números enteros. Vamos realizando divisiones hasta obtener un resto nulo. El resto anterior es el máximo común divisor.

$$\begin{aligned}
p(x) &= q(x) \cdot c_1(x) + r_1(x) \\
q(x) &= r_1(x) \cdot c_2(x) + r_2(x) \\
r_1(x) &= r_2(x) \cdot c_3(x) + r_3(x) \\
&\dots\dots\dots \\
r_{i-2}(x) &= r_{i-1}(x) \cdot c_i(x) + r_i(x) \\
&\dots\dots\dots \\
r_{k-2}(x) &= r_{k-1}(x) \cdot c_k(x) + r_k(x) \\
r_{k-1}(x) &= r_k(x) \cdot c_{k+1}(x) + 0
\end{aligned}$$

Sin embargo, el polinomio $r_k(x)$ no tiene por qué ser mónico, luego el resultado final, $r_k(x)$, no sería el máximo común divisor de $p(x)$ y $q(x)$. Necesitamos multiplicar por el inverso del coeficiente líder para obtener el máximo común divisor.

El algoritmo EUCLIDES del capítulo anterior vale ahora para el cálculo del máximo común divisor de dos polinomios con coeficientes en un cuerpo. Únicamente, al final hay que multiplicar el resultado por el inverso del coeficiente líder de $p(x)$.

En el caso de que los dos polinomios, $p(x)$ y $q(x)$ fueran nulos, el algoritmo daría error.

Algoritmo EUCLIDES($p(x), q(x)$)

Entrada: $p(x), q(x) \in K[x]$

Salida: $d(x) = \text{mcd}(p(x), q(x))$

Mientras $q(x) \neq 0$

$(p(x), q(x)) := (q(x), p(x) \bmod q(x))$

$a = \text{c.l.}(p(x))^{-1}$.

$p(x) := a \cdot p(x)$.

Devuelve $p(x)$

Ejemplo 3.2.7. Vamos a calcular en $\mathbb{Q}[x]$ el máximo común divisor de $x^3 - x + 3$ y $x^3 + x^2 + 1$.

$$\begin{array}{rclcl}
x^3 - x + 3 & = & (x^3 + x^2 + 1) & 1 & + & (-x^2 - x + 2) \\
x^3 + x^2 + 1 & = & (-x^2 - x + 2) & (-x) & + & 2x + 1 \\
-x^2 - x + 2 & = & (2x + 1) & \left(-\frac{1}{2}x - \frac{1}{4}\right) & + & \frac{9}{4} \\
2x + 1 & = & \frac{9}{4} & \left(\frac{8}{9}x + \frac{4}{9}\right) & + & 0
\end{array}$$

Luego un máximo común divisor de $x^3 - x + 3$ y $x^3 + x^2 + 1$ es $\frac{9}{4}$. Multiplicamos por $\frac{4}{9}$ y obtenemos que $\text{mcd}(x^3 - x + 3, x^3 + x^2 + 1) = 1$.

$p(x)$	$q(x)$	a
$x^3 - x + 3$	$x^3 + x^2 + 1$	
$x^3 + x^2 + 1$	$-x^2 - x + 2$	
$-x^2 - x + 2$	$2x + 1$	
$2x + 1$	$\frac{9}{4}$	
$\frac{9}{4}$	0	$\frac{4}{9}$
1		

El teorema de Bezout se tiene también en el caso de los polinomios.

Teorema 3.2.3. Sean $p(x), q(x) \in K[x]$, y sea $d(x) = \text{mcd}(p(x), q(x))$. Entonces existen $u(x), v(x) \in K[x]$ tales que $d(x) = p(x) \cdot u(x) + q(x) \cdot v(x)$

La demostración del teorema, así como el algoritmo para calcular $u(x)$ y $v(x)$ es análogo al hecho en el caso de los números enteros. Hay que tener en cuenta que al final, hay que multiplicar el resultado por el inverso del coeficiente líder.

Algoritmo BEZOUT($p(x), q(x)$)

Entrada: $p(x), q(x) \in K[x]$

Salida: $(d(x), u(x), v(x))$: $d(x) = \text{mcd}(p(x), q(x))$; $d(x) = p(x) \cdot u(x) + q(x) \cdot v(x)$

Si $q(x) = 0$

$a := \text{c.l.}(p(x))^{-1}$

Devuelve $(a \cdot p(x), a, 0)$;

Fin

$r_{-1}(x) := p(x), r_0(x) := q(x)$.

$u_{-1}(x) := 1, u_0(x) := 0$.

$v_{-1}(x) := 0, v_0(x) := 1$.

$i := 1$.

$r_1(x) := r_{-1}(x) \bmod r_0(x)$

Mientras $r_i(x) \neq 0$

$c_i(x) := r_{i-2}(x) \text{ div } r_{i-1}(x)$.

$u_i(x) := u_{i-2}(x) - u_{i-1}(x) \cdot c_i(x)$.

$v_i(x) := v_{i-2}(x) - v_{i-1}(x) \cdot c_i(x)$.

$i := i + 1$.

$r_i(x) := r_{i-2}(x) \bmod r_{i-1}(x)$.

$a := \text{c.l.}(r_{i-1}(x))^{-1}$

$r(x) := a \cdot r_{i-1}(x); u(x) := a \cdot u_{i-1}(x); v(x) := a \cdot v_{i-1}(x)$.

Devuelve $(r(x), u(x), v(x))$.

Fin

Ejemplo 3.2.8.

1. Vamos a expresar $\text{mcd}(x^3 - x + 3, x^3 + x^2 + 1)$ en función de los polinomios $x^3 - x + 3$ y $x^3 + x^2 + 1$.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		$x^3 - x + 3$		1	0
0		$x^3 + x^2 + 1$		0	1
1		$-x^2 - x + 2$	1	1	-1
2		$2x - 1$	$-x$	x	$-x + 1$
3		$\frac{9}{4}$	$\frac{-1}{2}x - \frac{1}{4}$	$\frac{1}{2}x^2 + \frac{1}{4}x + 1$	$\frac{-1}{2}x^2 + \frac{1}{4}x - \frac{3}{4}$
4	$\frac{4}{9}$	0			
		1		$\frac{2}{9}x^2 + \frac{1}{9}x + \frac{4}{9}$	$\frac{-2}{9}x^2 + \frac{1}{9}x - \frac{3}{9}$

Aquí vemos cómo se han obtenido las dos últimas columnas:

$$1 = 1 - 1 \cdot 0$$

$$x = 0 - (-x) \cdot 1$$

$$\frac{1}{2}x^2 + \frac{1}{4}x + 1 = 1 - \left(\frac{-1}{2}x - \frac{1}{4}\right) \cdot x$$

$$-1 = 0 - 1 \cdot 1$$

$$-x + 1 = 1 - (-x) \cdot (-1)$$

$$\frac{-1}{2}x^2 + \frac{1}{4}x - \frac{3}{4} = -1 - \left(\frac{-1}{2}x - \frac{1}{4}\right) \cdot (-x + 1)$$

Nótese que se verifica que

$$1 = (x^3 - x + 3) \left(\frac{2}{9}x^2 + \frac{1}{9}x + \frac{4}{9} \right) + (x^3 + x^2 + 1) \left(\frac{-2}{9}x^2 + \frac{1}{9}x - \frac{3}{9} \right)$$

2. Sean $p(x) = x^5 + 2x^4 + x^2 + 2x + 2$, $q(x) = x^5 + 2x^3 + x^2 + x + 1 \in \mathbb{Z}_3[x]$. Vamos a calcular su máximo común divisor y a expresarlo en función de $p(x)$ y $q(x)$.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		$x^5 + 2x^4 + x^2 + 2x + 2$		1	0
0		$x^5 + 2x^3 + x^2 + x + 1$		0	1
1		$2x^4 + x^3 + x + 1$	1	1	2
2		$2x^2 + 2$	$2x + 2$	$x + 1$	$2x$
3	2	0			
		$\mathbf{x^2 + 1}$		$\mathbf{2x + 2}$	\mathbf{x}

Luego $\text{mcd}(x^5 + 2x^4 + x^2 + 2x + 2, x^5 + 2x^3 + x^2 + x + 1) = x^2 + 1$ y

$$x^2 + 1 = (x^5 + 2x^4 + x^2 + 2x + 2)(2x + 2) + (x^5 + 2x^3 + x^2 + x + 1)(x)$$

3. En $\mathbb{Z}[x]$ se tiene que $\text{mcd}(x, 2) = 1$. Sin embargo no es posible encontrar $u(x), v(x) \in \mathbb{Z}[x]$ tales que $x \cdot u(x) + 2 \cdot v(x) = 1$.

Los Corolarios 2.3.2, 2.3.3 y 2.3.4, así como la Proposición 2.3.1 pueden ahora trasladarse al contexto de polinomios con coeficientes en un cuerpo.

También las Proposiciones 2.4.1 y 2.4.2 son válidas para polinomios.

Más precisamente, sean $a(x), b(x), c(x) \in K[x]$. Entonces la ecuación $a(x)u(x) + b(x)v(x) = c(x)$ tiene solución si, y sólo si, $\text{mcd}(a(x), b(x)) \mid c(x)$.

Si $u_0(x), v_0(x)$ es una tal solución, y $d(x) = \text{mcd}(a(x), b(x))$, entonces todas las soluciones son de la forma:

$$\begin{aligned} u(x) &= u_0(x) + p(x) \frac{b(x)}{d(x)} \\ v(x) &= v_0(x) - p(x) \frac{a(x)}{d(x)} \end{aligned} \quad p(x) \in K[x]$$

Ejemplo 3.2.9. Vamos a hallar todas las parejas de polinomio $u(x), v(x) \in \mathbb{Z}_3[x]$ que satisfacen la ecuación

$$(x^5 + 2x^3 + 2) \cdot u(x) + (x^5 + 2x^4 + 2x^3 + 1) \cdot v(x) = x^4 + 2x^2 + 2x + 2$$

Para esto, vemos en primer lugar si existe alguno. Esto ocurre si, y sólo si, $x^4 + 2x^2 + 2x + 2$ es múltiplo de $\text{mcd}(x^5 + 2x^3 + 2, x^5 + 2x^4 + 2x^3 + 1)$.

a	$a(x)$	$b(x)$	$c(x)$
	$x^5 + 2x^3 + 2$	$x^5 + 2x^4 + 2x^3 + 1$	1
	$x^5 + 2x^4 + 2x^3 + 1$	$x^4 + 1$	$x + 2$
	$x^4 + 1$	$2x^3 + 2x + 2$	$2x$
	$2x^3 + 2x + 2$	$2x^2 + 2x + 1$	
2	$2x^2 + 2x + 1$	0	
	$x^2 + x + 2$		

luego $\text{mcd}(x^5 + 2x^3 + 2, x^5 + 2x^4 + 2x^3 + 1) = x^2 + x + 2$, y como $x^4 + 2x^2 + 2x + 2 = (x^2 + x + 2)(x^2 + 2x + 1)$, es decir, $(x^2 + x + 2) \mid (x^4 + 2x^2 + 2x + 2)$ sabemos que podemos encontrar parejas de polinomio $u(x), v(x)$ que sean solución de la ecuación anterior.

Buscamos dos polinomios $u_0(x), v_0(x)$ que sean solución. Para eso, completamos la tabla anterior.

a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
	$x^5 + 2x^3 + 2$		1	0
	$x^5 + 2x^4 + 2x^3 + 1$		0	1
	$x^4 + 1$	1	1	2
	$2x^3 + 2x + 2$	$x + 2$	$2x + 1$	x
	$2x^2 + 2x + 1$	$2x$	$2x^2 + x + 1$	$x^2 + 2$
2	0			
	$\mathbf{x^2 + x + 2}$		$\mathbf{x^2 + 2x + 2}$	$\mathbf{2x^2 + 1}$

Tomamos entonces

$$\begin{aligned} u_0(x) &= (x^2 + 2x + 2) \cdot (x^2 + 2x + 1) = x^4 + x^3 + x^2 + 2 \\ v_0(x) &= (2x^2 + 1) \cdot (x^2 + 2x + 1) = 2x^4 + x^3 + 2x + 1 \end{aligned}$$

Puesto que

$$(x^5 + 2x^3 + 2) \operatorname{div} (x^2 + x + 2) = x^3 + 2x^2 + x + 2$$

$$(x^5 + 2x^4 + 2x^3 + 1) \operatorname{div} (x^2 + x + 2) = x^3 + x^2 + 2x + 2$$

tenemos que la solución general es

$$\begin{aligned} u(x) &= x^4 + x^3 + x^2 + 2 + (x^3 + x^2 + 2x + 2) \cdot p(x) \\ v(x) &= 2x^4 + x^3 + 2x + 1 + 2(x^3 + 2x^2 + x + 2) \cdot p(x) \end{aligned} \quad p(x) \in \mathbb{Z}_3[x]$$

3.3. Factorización de polinomios

En esta sección veremos como los polinomios con coeficientes en un cuerpo se pueden factorizar como producto de irreducibles.

3.3.1. Polinomios irreducibles.

Comenzamos con la definición de polinomios irreducibles.

Definición 46. Sea $p(x) \in K[x]$ no constante. Se dice que $p(x)$ es irreducible si sus únicos divisores son los polinomios constantes (no nulos) y los polinomios de la forma $a \cdot p(x) : a \in K^*$.

Sea $p(x) \in \mathbb{Z}[x]$, $p(x) \neq 0, 1, -1$. Se dice que $p(x)$ es irreducible si sus únicos divisores son ± 1 y $\pm p(x)$.

Si $p(x)$ no es irreducible, se dice que es reducible.

Observación: Nótese que si $p(x) \in K[x]$ es reducible y $\operatorname{gr}(p(x)) = n$ entonces $p(x)$ tiene un divisor no constante de grado menor o igual que $\frac{n}{2}$.

Ejemplo 3.3.1.

1. Cualquier polinomio de grado 1 en $K[x]$ es irreducible. Sin embargo, el polinomio $p(x) = 2x + 2$ es reducible en $\mathbb{Z}[x]$, pues $2|p(x)$ y $x+1|p(x)$.
2. El polinomio $x^3 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible. Por la observación anterior debe tener un divisor de grado menor o igual que $\frac{3}{2}$. Los únicos polinomios en esas condiciones son x y $x+1$, y ninguno de ellos divide a $x^3 + x + 1$.
3. Dado $p(x) = ax^2 + bx + c \in \mathbb{R}[x]$ entonces $p(x)$ es irreducible si, y sólo si, $b^2 - 4ac < 0$.

Al igual que en el caso de \mathbb{Z} se tiene ahora:

Proposición 3.3.1. *Sea $p(x) \in K[x]$ no constante. Entonces:*

$$p(x) \text{ es irreducible} \iff (p(x)|q_1(x) \cdot q_2(x) \implies p(x)|q_1(x) \text{ ó } p(x)|q_2(x))$$

Con esta proposición estamos ya en condiciones de dar el teorema de factorización.

Teorema 3.3.1. *Sea K un cuerpo, y $p(x) \in K[x]$ no constante. Entonces $p(x)$ se expresa de forma única como*

$$p(x) = ap_1(x)p_2(x) \cdots p_k(x)$$

donde $a \in K$ y $p_i(x)$ es un polinomio mónico e irreducible.

La demostración es similar a la que se hizo del teorema fundamental de la aritmética.

En $\mathbb{Z}_8[x]$ se tiene que $x^2 + 7 = (x+1)(x+7) = (x+3)(x+5)$. Vemos entonces que podemos factorizar un polinomio de dos formas distintas. Sin embargo, puesto que \mathbb{Z}_8 no es un cuerpo, este ejemplo no está en contradicción con la afirmación de la factorización única que nos da el teorema 3.3.1.

En el caso de polinomios con coeficientes en \mathbb{Z} la situación es algo diferente, pues en general no es posible expresar un polinomio irreducible como una constante por un polinomio mónico. Por ejemplo, $2x^2 + 4x + 1$ es irreducible. Si lo expresamos como una constante por un polinomio mónico nos queda $2(x^2 + 2x + \frac{1}{2})$ que no pertenece a $\mathbb{Z}[x]$. El papel de polinomio mónico lo juega aquí lo que se llama polinomio primitivo.

Definición 47. *Sea $p(x) \in \mathbb{Z}[x]$ no nulo. Se llama contenido de $p(x)$ al máximo común divisor de sus coeficientes. Es decir, si $p(x) = a_n x^n + \cdots + a_1 x + a_0$, entonces*

$$c(p(x)) = \text{mcd}(a_0, a_1, \dots, a_n)$$

Un polinomio se dice primitivo si su contenido vale 1.

Obviamente, dado $p(x) \in \mathbb{Z}[x]$, entonces $p(x)$ se expresa como $p(x) = c(p(x)) \cdot p_1(x)$, donde $p_1(x)$ es un polinomio primitivo. Más en general, si $p(x) \in \mathbb{Q}[x]$, existe $\frac{a}{b} \in \mathbb{Q}$ y $p_1(x) \in \mathbb{Z}[x]$ primitivo tal que $p(x) = \frac{a}{b} p_1(x)$.

Ejemplo 3.3.2. *El contenido del polinomio $6x^3 + 9x^2 - 15x + 12$ es 3, pues $\text{mcd}(6, 9, -15, 12) = 3$. Se tiene entonces que $p(x) = 3 \cdot (2x^3 + 3x^2 - 5x + 4)$. Fácilmente se comprueba que $2x^3 + 3x^2 - 5x + 4$ es primitivo.*

Consideramos el polinomio $p(x) = 7x^3 - \frac{7}{5}x^2 + \frac{14}{3}x - \frac{7}{3} \in \mathbb{Q}[x]$. Multiplicamos por el mínimo común múltiplo de los denominadores, que es 15, y nos queda:

$$p(x) = \frac{1}{15}(105x^3 - 21x^2 + 70x - 35)$$

y como este último polinomio tiene contenido igual a 7 resulta que

$$p(x) = \frac{7}{15}(15x^3 - 3x^2 + 10x - 5)$$

El teorema de factorización de polinomios en $\mathbb{Z}[x]$ dice:

Teorema 3.3.2. *Sea $q(x) \in \mathbb{Z}[x]$, $q(x) \neq 0, 1, -1$. Entonces $q(x)$ se factoriza como*

$$q(x) = p_1 \cdots p_r q_1(x) \cdots q_s(x)$$

donde p_i son números enteros primos y $q_j(x)$ son polinomios primitivos irreducibles en $\mathbb{Q}[x]$.

Más adelante estudiaremos esto con un poco más de detalle.

3.3.2. Raíces de polinomios.

Sabemos que si tenemos $p(x) \in K[x]$, entonces $p(x)$ se expresa de forma única como producto de irreducibles. Sin embargo, en general no es fácil encontrar estos irreducibles. Existen resultados que permiten encontrar esta factorización cuando $K = \mathbb{Z}_p$ (algoritmo de Berlekamp), o $K = \mathbb{Q}$ (método de Kronecker o lema de Hensel) que se escapan de los objetivos de estas notas. Nosotros vamos a estudiar los métodos más sencillos.

A la hora de encontrar de encontrar los divisores irreducibles de un polinomio vamos a comenzar por los más simples: los de grado 1. Por tanto, vamos a buscar divisores de la forma $x - a$ con $a \in K$. Por el teorema 3.2.1 sabemos que encontrar un divisor de la forma $x - a$ es equivalente a encontrar una raíz $x = a$. En este apartado nos vamos a dedicar a ver cómo encontrar las raíces de polinomios.

Vamos a distinguir según el cuerpo en el que estemos trabajando.

Raíces de polinomios con coeficientes complejos.

Comenzamos con el caso $K = \mathbb{C}$. El teorema fundamental del álgebra nos dice que todo polinomio no constante con coeficientes complejos tiene al menos una raíz.

Si $p(x) \in \mathbb{C}[x]$ y a_1 es una raíz, entonces $p(x) = (x - a_1) \cdot p_1(x)$. Si ahora le volvemos a aplicar el mismo resultado a $p_1(x)$ tendremos $p(x) = (x - a_1) \cdot (x - a_2) \cdot p_2(x)$ (donde a_2 podría ser igual a a_1). Repitiendo el proceso, tenemos que $p(x) = a \cdot (x - a_1) \cdot (x - a_2) \cdots (x - a_n)$. Es decir, todo polinomio de grado n con coeficientes complejos se descompone como producto de n irreducibles de grado 1 (algunos podrían aparecer repetidos).

Por ejemplo, el polinomio $p(x) = x^3 - 2x^2 + x - 2$ tiene a $x = i$ como raíz. Si dividimos por $x - i$ nos queda $p(x) = (x - i) \cdot (x^2 + (-2 + i)x - 2i)$. Este tiene a $x = -i$ como raíz. Volviendo a dividir tenemos $p(x) = (x - i) \cdot (x + i) \cdot (x - 2)$.

El problema es que no tenemos forma de determinar las raíces complejas de un polinomio salvo algunos casos muy concretos.

Raíces de polinomios con coeficientes reales.

Si $p(x)$ es un polinomio con coeficientes reales de grado impar, sabemos, por el teorema de Bolzano, que tiene al menos una raíz real (pues los límites de la función $p(x)$ en $+\infty$ y $-\infty$ tienen signo distinto).

Por ejemplo, si $p(x) = x^3 - 7x^2 + 5x - 3$, entonces el límite cuando $x \rightarrow +\infty$ es $+\infty$ mientras que el límite cuando $x \rightarrow -\infty$ es $-\infty$. Luego debe haber algún punto en el que $p(x)$ valga cero. De hecho, $p(6) = -9$ y $p(7) = 32$, luego $p(x)$ tiene una raíz en el intervalo $]6, 7[$.

Pero al igual que antes, no tenemos forma de calcular esa raíz (bueno, podríamos aproximarla utilizando algún método numérico para tal efecto).

Para polinomios de grado 2, podemos encontrar las raíces con la conocida expresión $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Por ejemplo, el polinomio $x^2 - x - 1$ tiene como raíces a $x_1 = \frac{1+\sqrt{5}}{2}$ (número áureo) y $x_2 = \frac{1-\sqrt{5}}{2}$. Por tanto, tenemos que

$$x^2 - x - 1 = \left(x - \frac{1 + \sqrt{5}}{2}\right) \cdot \left(x - \frac{1 - \sqrt{5}}{2}\right)$$

Cuando decimos que una raíz es $\frac{1+\sqrt{5}}{2}$ tampoco hemos calculado una raíz del polinomio. Simplemente hemos puesto una raíz del polinomio $x^2 - x - 1$ en función de una raíz del polinomio $x^2 - 5$, y a esta raíz le hemos puesto un nombre ($\sqrt{5}$). Pero lo único que podemos conseguir es una aproximación de ese número con tanta precisión como queramos, al igual que cuando hablábamos de una raíz de $x^3 - 7x^2 + 5x - 3$.

Si tenemos ahora un polinomio $p(x) \in \mathbb{R}[x]$ que no tiene raíces reales, sabemos que tiene al menos una raíz compleja $\alpha = a + bi$. En tal caso, $\bar{\alpha} = a - bi$ es también una raíz de $p(x)$, y $(x - \alpha) \cdot (x - \bar{\alpha})$ es un divisor de $p(x)$. Como ese producto tiene los coeficientes reales (pues vale $(x - a)^2 + b^2$), podemos asegurar que $p(x)$ tiene un divisor de grado 2.

Deducimos entonces que todo polinomio irreducible real, o es de grado uno, o es de grado 2 y no tiene raíces reales.

Ejemplo 3.3.3.

1. Sea $p(x) = x^3 - 1$. Es claro que $x = 1$ es una raíz de este polinomio. Sus raíces complejas son las tres raíces de la unidad, que son

$$\cos(0) + i \operatorname{sen}(0) = 1; \quad \omega = \cos\left(\frac{2\pi}{3}\right) + i \operatorname{sen}\left(\frac{2\pi}{3}\right) = \frac{-1}{2} + i \frac{\sqrt{3}}{2}; \quad \bar{\omega} = \omega^2 = \cos\left(\frac{4\pi}{3}\right) + i \operatorname{sen}\left(\frac{4\pi}{3}\right) = \frac{-1}{2} - i \frac{\sqrt{3}}{2}$$

Por tanto, su factorización en $\mathbb{C}[x]$ es $p(x) = (x-1)(x-\omega)(x-\bar{\omega})$.

El producto $(x-\omega)(x-\bar{\omega})$ vale x^2+x+1 , que tiene los coeficientes reales. Por tanto, la factorización de $p(x)$ en $\mathbb{R}[x]$ es $p(x) = (x-1)(x^2+x+1)$.

2. Sea ahora $p(x) = x^8 - 1$. Este polinomio tiene 8 raíces complejas, que son:

$$\begin{aligned} \alpha_0 &= \cos(0) + i \operatorname{sen}(0) = 1 & \alpha_1 &= \cos\left(\frac{2\pi}{8}\right) + i \operatorname{sen}\left(\frac{2\pi}{8}\right) = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \\ \alpha_2 &= (\alpha_1)^2 = \cos\left(\frac{4\pi}{8}\right) + i \operatorname{sen}\left(\frac{4\pi}{8}\right) = i & \alpha_3 &= (\alpha_1)^3 = \cos\left(\frac{6\pi}{8}\right) + i \operatorname{sen}\left(\frac{6\pi}{8}\right) = \frac{-\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \\ \alpha_4 &= (\alpha_1)^4 = \cos\left(\frac{8\pi}{8}\right) + i \operatorname{sen}\left(\frac{8\pi}{8}\right) = -1 & \alpha_5 &= (\alpha_1)^5 = \cos\left(\frac{10\pi}{8}\right) + i \operatorname{sen}\left(\frac{10\pi}{8}\right) = \frac{-\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \\ \alpha_6 &= (\alpha_1)^6 = \cos\left(\frac{12\pi}{8}\right) + i \operatorname{sen}\left(\frac{12\pi}{8}\right) = -i & \alpha_7 &= (\alpha_1)^7 = \cos\left(\frac{14\pi}{8}\right) + i \operatorname{sen}\left(\frac{14\pi}{8}\right) = \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \end{aligned}$$

Notemos como $\bar{\alpha}_1 = \alpha_7$, $\bar{\alpha}_2 = \alpha_6$ y $\bar{\alpha}_3 = \alpha_5$.

La factorización de $p(x)$ en $\mathbb{C}[x]$ sería $\prod_{i=0}^7 (x - \alpha_i)$.

Podemos ver como $(x - \alpha_1)(x - \alpha_7) = x^2 - \sqrt{2}x + 1$, $(x - \alpha_2)(x - \alpha_6) = (x - i)(x + i) = x^2 + 1$ y $(x - \alpha_3)(x - \alpha_5) = x^2 + \sqrt{2}x + 1$. La factorización de $p(x)$ en $\mathbb{R}[x]$ es entonces

$$p(x) = (x-1)(x+1)(x^2+1)(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$$

Y por último, puesto que $(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1) = x^4 + 1$, la factorización de $p(x)$ en $\mathbb{Q}[x]$ es

$$p(x) = (x-1)(x+1)(x^2+1)(x^4+1)$$

Raíces de polinomios con coeficientes en \mathbb{Z}_p .

En este caso, y puesto que el número de elementos de \mathbb{Z}_p es finito, la forma que tenemos de buscar las raíces es probando con los distintos elementos de \mathbb{Z}_p .

Por tanto, si $q(x) \in \mathbb{Z}_p[x]$, para ver si tiene raíces, lo que tenemos que hacer es evaluar el polinomio en los distintos elementos de \mathbb{Z}_p . Es decir, calculamos $q(0), q(1), \dots, q(p-1)$, y comprobamos si en algún caso nos ha dado cero.

Ejemplo 3.3.4. 1. Sea $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Entonces $p(0) = 1$ y $p(1) = 1$. Como $\mathbb{Z}_2 = \{0, 1\}$, el polinomio $p(x)$ no tiene raíces.

2. Sea ahora $p(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$. Ahora se tiene que $p(1) = 0$, luego $x = 1$ es una raíz. Probamos a dividir por $x - 1$.

$$\begin{array}{r|rrrr} & 1 & 0 & 1 & 1 \\ 1 & & 1 & 1 & 2 \\ \hline & 1 & 1 & 2 & 0 \end{array}$$

Luego $p(x) = (x+2) \cdot (x^2+x+2)$. Puede comprobarse fácilmente que x^2+x+2 no tiene raíces.

3. Sea $p(x) = x^4 + 3x^3 + 2x^2 + 6x + 5 \in \mathbb{Z}_7[x]$. Vamos a encontrar sus raíces. Para eso, vamos a ir probando por los distintos elementos de \mathbb{Z}_7 . Claramente, $p(0) = 5 \neq 0$.

$$\begin{array}{r|rrrrr} & 1 & 3 & 2 & 6 & 5 \\ 1 & & 1 & 4 & 6 & 5 \\ \hline & 1 & 4 & 6 & 5 & 3 \end{array} \quad \begin{array}{r|rrrrr} & 1 & 3 & 2 & 6 & 5 \\ 2 & & 2 & 3 & 3 & 4 \\ \hline & 1 & 5 & 5 & 2 & 2 \end{array} \quad \begin{array}{r|rrrrr} & 1 & 3 & 2 & 6 & 5 \\ 3 & & 3 & 4 & 4 & 2 \\ \hline & 1 & 6 & 6 & 3 & 0 \end{array}$$

Luego $x = 3$ es una raíz, y $p(x) = (x - 3) \cdot (x^3 + 6x^2 + 6x + 3)$. Ahora seguimos buscando raíces, pero lo hacemos con el polinomio $x^3 + 6x^2 + 6x + 3$. Con $x = 0$, $x = 1$ y $x = 2$ ya no tenemos que probar, pues lo hemos hecho antes.

$$\begin{array}{c|cccc} & 1 & 6 & 6 & 3 \\ 3 & & 3 & 6 & 1 \\ \hline & 1 & 2 & 5 & 4 \end{array} \quad \begin{array}{c|cccc} & 1 & 6 & 6 & 3 \\ 4 & & 4 & 5 & 2 \\ \hline & 1 & 3 & 4 & 5 \end{array} \quad \begin{array}{c|cccc} & 1 & 6 & 6 & 3 \\ 5 & & 5 & 6 & 4 \\ \hline & 1 & 4 & 5 & 0 \end{array}$$

Y vemos que $x = 5$ es otra raíz. Tenemos entonces que $p(x) = (x - 3) \cdot (x - 5) \cdot (x^2 + 4x + 5)$. Continuamos ahora con $x^2 + 4x + 5$.

$$\begin{array}{c|ccc} & 1 & 4 & 5 \\ 5 & & 5 & 3 \\ \hline & 1 & 2 & 1 \end{array} \quad \begin{array}{c|ccc} & 1 & 4 & 5 \\ 6 & & 6 & 4 \\ \hline & 1 & 3 & 2 \end{array}$$

Y por tanto, $p(x)$ no tiene más raíces. Tendríamos entonces la siguiente factorización del polinomio $p(x)$:

$$p(x) = (x + 4) \cdot (x + 2) \cdot (x^2 + 4x + 5).$$

Raíces de polinomios con coeficientes en \mathbb{Q} .

Vamos a terminar este apartado viendo cómo encontrar las raíces racionales de un polinomio con coeficientes en \mathbb{Q} .

Notemos en primer lugar que si $p(x) \in \mathbb{Q}[x]$, entonces podemos multiplicar $p(x)$ por una constante r de forma que el polinomio $r \cdot p(x)$ tenga los coeficientes enteros y sea primitivo (ver definición 47). Y las raíces de $p(x)$ y $r \cdot p(x)$ son las mismas.

Por tanto, tomamos $p(x) \in \mathbb{Z}[x]$ primitivo, y nos proponemos calcular sus raíces racionales.

Tenemos el siguiente resultado.

Proposición 3.3.2. Sea $q(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio con coeficientes en \mathbb{Z} y primitivo, y sea $\frac{a}{b} \in \mathbb{Q}$. Supongamos que $\text{mcd}(a, b) = 1$. Entonces, si $\frac{a}{b}$ es una raíz de $q(x)$, se verifica que $a|a_0$ y $b|a_n$.

Demostración: Por ser $\frac{a}{b}$ una raíz de $q(x)$ se tiene que $q\left(\frac{a}{b}\right) = 0$, es decir,

$$a_n \left(\frac{a}{b}\right)^n + \cdots + a_1 \frac{a}{b} + a_0 = 0 \implies a_n a^n + a_{n-1} a^{n-1} b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0,$$

y de aquí se tiene, por una parte que

$$a_0 b^n = -a(a_n a^{n-1} + a_{n-1} a^{n-2} b + \cdots + a_1 a b^{n-1}),$$

lo que implica que $a|(a_0 b^n)$, y por tanto $a|a_0$ (ya que $\text{mcd}(a, b) = 1$. Ver corolario 2.3.4); y por otra parte que

$$a_n a^n = -b(a_{n-1} a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}),$$

lo que implica que $b|a_n$. ■

Ejemplo 3.3.5. Consideramos el polinomio $q(x) = 2x^3 + 3x^2 - 5x + 1$. Sus posibles raíces racionales son ± 1 y $\pm \frac{1}{2}$, pues el numerador tiene que ser un divisor de 1 y el denominador un divisor de 2. Evaluamos en esos puntos y obtenemos:

$$q(1) = 1 \quad q(-1) = 7 \quad q\left(\frac{1}{2}\right) = \frac{-1}{2} \quad q\left(\frac{-1}{2}\right) = 4$$

luego $q(x)$ no tiene raíces racionales.

Aunque esta proposición nos acota bastante el número de posibles raíces, haciendo uso únicamente de la proposición éste podría ser bastante elevado.

Ejemplo 3.3.6. Sea $q(x) = 6x^4 + 11x^3 - 19x^2 + 18x - 8$. Si nos atenemos a la proposición 3.3.3 las posibles raíces de $q(x)$ son

Con denominador 1: 1, 2, 4, 8, -1, -2, -4, -8.

Con denominador 2: $\frac{1}{2}, \frac{-1}{2}$ (pues las otras ya las hemos considerado).

Con denominador 3: $\frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{8}{3}, \frac{-1}{3}, \frac{-2}{3}, \frac{-4}{3}, \frac{-8}{3}$.

Con denominador 6: $\frac{1}{6}, \frac{-1}{6}$.

Y vemos que hay un total de 20 posibles raíces por las que hay que probar.

El siguiente resultado nos permite reducir aún más las posibles raíces de un polinomio con coeficientes en \mathbb{Z} .

Proposición 3.3.3. Sea $q(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Supongamos que $\frac{a}{b}$ es una raíz de $q(x)$, con $\text{mcd}(a, b) = 1$. Entonces, para cualquier $c \in \mathbb{Z}$ se verifica que $(bc - a) | p(c)$.

La demostración de esta proposición se hará más adelante.

Si en la proposición anterior tomamos $c = 0$ obtenemos que $a | a_0$.

Si tomamos $c = 1$ obtenemos que $(b - a) | p(1)$.

Si tomamos $c = -1$ obtenemos que $(b + a) | p(-1)$.

Ejemplo 3.3.7. Retomamos el polinomio $q(x) = 6x^4 + 11x^3 - 19x^2 + 18x - 8$ del ejemplo anterior. Entonces $q(1) = 8$ y $q(-1) = -50$.

Tenemos entonces que si $\frac{a}{b}$ es una raíz de $q(x)$ entonces $b - a$ es un divisor de 8. Podemos entonces eliminar de la lista de posibles raíces las siguientes: 1 (esta pues ya hemos calculado $q(1)$, y nos ha dado distinto de cero), 4 (4 es una fracción con numerador 4 y denominador 1, y la diferencia de ambos es 3, que no es divisor de 8), 8 (aquí tenemos que $b - a = -7$), -2, -4, -8, $\frac{-1}{2}$, $\frac{-2}{3}$, $\frac{-4}{3}$, $\frac{8}{3}$, $\frac{-8}{3}$, $\frac{1}{6}$, $\frac{-1}{6}$.

Nos quedan entonces:

$$2 \quad -1 \quad \frac{1}{2} \quad \frac{1}{3} \quad \frac{-1}{3} \quad \frac{2}{3} \quad \frac{4}{3}$$

Si ahora imponemos que $a + b$ sea un divisor de 50 nos quedan únicamente dos posibles raíces, que son $\frac{-1}{3}$ y $\frac{2}{3}$.

$$\begin{array}{c|cccccc} \frac{-1}{3} & 6 & 11 & -19 & 18 & -8 \\ & & -2 & -3 & \frac{22}{3} & \frac{-76}{3} \\ \hline & 6 & 9 & -22 & \frac{76}{3} & \frac{-148}{9} \end{array} \quad \begin{array}{c|cccccc} \frac{2}{3} & 6 & 11 & -19 & 18 & -8 \\ & & 4 & 10 & -6 & 8 \\ \hline & 6 & 15 & -9 & 12 & 0 \end{array}$$

de donde deducimos que $q(x) = (x - \frac{2}{3})(6x^3 + 15x^2 - 9x + 12) = (3x - 2)(2x^3 + 5x^2 - 3x + 4)$.

Y ahora podemos concluir que $2x^3 + 5x^2 + 3x + 4$ no tiene raíces. Por tanto, la única raíz de $q(x)$ es $\frac{2}{3}$.

Terminamos esta sección con un resultado muy sencillo pero que es útil a la hora de estudiar la posible irreducibilidad de polinomios.

Proposición 3.3.4. Sea $p(x) \in K[x]$ un polinomio de grado 2 ó 3. Entonces $p(x)$ es irreducible si, y sólo si, no tiene raíces.

Demostración: Es claro que si el polinomio es irreducible no tiene raíces, pues en tal caso tendría un divisor de grado uno.

Por otra parte, si el polinomio fuera reducible, vimos que tiene que tener un divisor de grado menor o igual a la mitad del grado de $p(x)$. Por tanto, debe tener un divisor de grado 1, lo que se traduce en que tiene una raíz. ■

Lo dicho en esta proposición vale únicamente para polinomios de grado 2 ó 3. Para polinomios de grado mayor no afirma nada.

Ejemplo 3.3.8.

1. Sea $p(x) = x^3 + \frac{5}{2}x^2 - 3x - \frac{3}{2} \in \mathbb{Q}[x]$. Vamos a estudiar si es reducible o irreducible, y en caso de ser reducible, encontrar su factorización.

Como es de grado 3, nos basta con encontrar sus raíces. Para eso, lo que hacemos es trabajar con $q(x) = 2 \cdot p(x) = 2x^3 + 5x^2 - 6x - 3$, que es primitivo. Las posibles raíces de este polinomio son, en principio, $1, -1, 3, -3, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}$.

Puesto que $q(1) = -2$, si $\frac{a}{b}$ es una raíz de $q(x)$, $a - b$ debe ser un divisor de 2. Esto nos elimina las posibilidades $1, -3, -\frac{1}{2}, -\frac{3}{2}$. Por tanto, las posibles raíces son $-1, 3, \frac{1}{2}$ y $\frac{3}{2}$.

Y ahora, dado que $q(-1) = 6$ podemos descartar $-1, 3$ y $\frac{3}{2}$. Luego la única posible raíz es $\frac{1}{2}$. Pero $q(\frac{1}{2}) = \frac{-9}{2} \neq 0$. Por tanto, el polinomio $q(x)$ no tiene raíces y es irreducible (también $p(x)$).

2. Sea $p(x) = x^4 + 2x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$. Entonces $p(0) = 2, p(1) = 1$ y $p(2) = 0$. Por tanto, 2 es una raíz y podemos dividir el polinomio por $x - 2 = x + 1$.

$$\begin{array}{c|cccc} & 1 & 2 & 2 & 0 & 2 \\ 2 & & 2 & 2 & 2 & 1 \\ \hline & 1 & 1 & 1 & 2 & 0 \end{array}$$

Luego $p(x) = (x+1) \cdot (x^3 + x^2 + x + 2)$. Este último polinomio es de grado 3 y no tiene raíces (ahora sólo habría que comprobar que 2 no es raíz), lo que nos dice que es irreducible.

3. Sea $p_1(x) = x^4 + 4x^3 + 4x^2 + 3$ y $p_2(x) = x^4 + 3x^3 + 3x^2 + x + 4$ dos polinomios con coeficientes en \mathbb{Z}_5 . Podemos comprobar que ninguno de ellos tiene raíces:

$$\begin{array}{ccccc} p_1(0) = 3 & p_1(1) = 2 & p_1(2) = 2 & p_1(3) = 3 & p_1(4) = 4 \\ p_2(0) = 4 & p_2(1) = 2 & p_2(2) = 3 & p_2(3) = 1 & p_2(4) = 4 \end{array}$$

Sin embargo, $p_1(x)$ es reducible, pues puede factorizarse como $(x^2 + x + 2) \cdot (x^2 + 3x + 4)$, mientras que $p_2(x)$ es irreducible.

3.3.3. Factores múltiples.

Sabemos que dado un polinomio $p(x) \in K[x]$, ese polinomio se puede expresar de forma única como producto de polinomios irreducibles. En esta factorización puede que aparezca alguno (o algunos) de los irreducibles repetidos. En tal caso, diremos que ese irreducible es un *factor múltiple* de $p(x)$.

Ya vimos (ver definición 44) lo que significa una raíz múltiple. Este concepto puede generalizarse a un polinomio irreducible de cualquier grado.

Definición 48. Sea $p(x) \in K[x]$ y $q(x) \in K[x]$ irreducible. Diremos que $q(x)$ es un factor de $p(x)$ de multiplicidad m si $p(x) = q(x)^m r(x)$ y $q(x)$ no es un divisor de $r(x)$.

Si $q(x)$ es un factor de multiplicidad mayor o igual que 2, diremos que $q(x)$ es un factor múltiple de $p(x)$.

Si $q(x)$ es un factor de $p(x)$ de multiplicidad 1, suele decirse que $q(x)$ es un factor simple de $p(x)$.

Es evidente que es lo mismo decir que a es una raíz de $p(x)$ de multiplicidad m a decir que $(x - a)$ es un factor de $p(x)$ de multiplicidad m .

Ejemplo 3.3.9. Sea $p(x) = x^9 + x^8 + x^7 + x^6 + x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$. Podemos ver que $x^2 + x + 1$ es factor de multiplicidad 3, pues $p(x) = (x^2 + x + 1)^3(x^3 + x + 1)$, y $x^2 + x + 1$ no es un divisor de $x^3 + x + 1$.

Un polinomio que no tenga factores múltiples es lo que se conoce como *libre de cuadrados*.

Definición 49. Sea $p(x) \in K[x]$. Se dice que $p(x)$ es libre de cuadrados si no existe $q(x) \in K[x]$, no constante, tal que $q(x)^2 | p(x)$.

Como ejercicio comprueba que esta definición es equivalente a decir que el polinomio $p(x)$ no tiene factores múltiples.

Lo que vamos a hacer a continuación es tratar de encontrar los factores múltiples de un polinomio. Para esto nos va a ser necesario estudiar la derivada de un polinomio. En este contexto la derivada de un polinomio es una forma de asociarle a un polinomio otro polinomio, pero no tiene ningún sentido de límite, ni de pendiente, etc.

Definición 50. Sea $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$. Se define la derivada de $p(x)$ como el polinomio

$$na_n x^{n-1} + \cdots + 2a_2 x + a_1$$

A dicho polinomio lo denotaremos como $D(p(x))$ o $p'(x)$.

Ejemplo 3.3.10.

1. Sea $p(x) = 2x^5 - 7x^3 + 3x^2 - 5x + 3 \in \mathbb{Q}[x]$. Entonces $p'(x) = 10x^4 - 21x^2 + 6x - 5$.
2. Sea $p(x) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$. En este caso se tiene que $p'(x) = 0$. Vemos como un polinomio no constante puede tener derivada nula.

Las propiedades de la derivada de polinomios recuerdan a las conocidas para la derivada de funciones reales. La demostración se deja como ejercicio.

Proposición 3.3.5. Sean $p(x), q(x) \in K[x]$, y $n \in \mathbb{N}$. Entonces:

- ▮ $D(p(x) + q(x)) = p'(x) + q'(x)$,
- ▮ $D(p(x) \cdot q(x)) = p'(x) \cdot q(x) + p(x) \cdot q'(x)$,
- ▮ $D(p(x)^n) = n \cdot p(x)^{n-1} p'(x)$.

La importancia de la derivada viene dada por el siguiente resultado.

Proposición 3.3.6. Sea $p(x) \in K[x]$. Entonces $p(x)$ es libre de cuadrados si, y sólo si, $\text{mcd}(p(x), p'(x)) = 1$.

Demostración:

Demostremos en primer lugar que si $\text{mcd}(p(x), p'(x)) = 1$ entonces $p(x)$ es libre de cuadrados, o, equivalentemente, si $p(x)$ no es libre de cuadrados entonces $\text{mcd}(p(x), p'(x)) \neq 1$.

Si $p(x)$ no es libre de cuadrados, entonces existen $q(x), r(x) \in K[x]$ tales que $p(x) = q(x)^2 r(x)$. Se tiene entonces que

$$p'(x) = D(q(x)^2 r(x) + q(x)^2 D(r(x))) = 2q(x)q'(x)r(x) + q(x)^2 r'(x) = q(x)(2q'(x)r(x) + q(x)r'(x)),$$

lo que implica que $q(x) | p'(x)$, y como $q(x) | p(x)$ se tiene que $q(x) | \text{mcd}(p(x), p'(x))$.

Recíprocamente, supongamos que $\text{mcd}(p(x), p'(x)) \neq 1$. Sea entonces $q(x)$ un polinomio irreducible divisor de $\text{mcd}(p(x), p'(x))$. Se tiene entonces que $p(x) = q(x)r(x)$. Derivamos:

$$p'(x) = q'(x)r(x) + q(x)r'(x)$$

Dado que $q(x) | p'(x)$ y $q(x) | q(x)r'(x)$ deducimos que $q(x) | q'(x)r(x)$, y al ser $q(x)$ irreducible tenemos dos opciones:

- 1. $q(x)|r(x)$. En este caso $r(x) = q(x)h(x)$, de donde $p(x) = q(x)^2h(x)$, es decir, $p(x)$ no es libre de cuadrados.
- 1. $q(x)|q'(x)$. Pero esta posibilidad sólo podría darse si $q'(x) = 0$. Sin embargo, veremos en un capítulo posterior que si $q'(x) = 0$ entonces $q(x)$ no es irreducible.

■

Corolario 3.3.1. Sea $p(x) \in K[x]$ y $a \in K$ una raíz de $p(x)$. Entonces a es una raíz múltiple de $p(x)$ si, y sólo si, $p'(a) = 0$.

Ejemplo 3.3.11.

1. Hemos visto que el polinomio $p(x) = x^9 + x^8 + x^7 + x^6 + x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$ no es libre de cuadrados, pues tenía un factor triple. Su derivada vale $p'(x) = x^8 + x^6 + x^4$. Vamos a calcular el máximo común divisor de $p(x)$ y su derivada. Para ello, usaremos el algoritmo de Euclides.

$$x^9 + x^8 + x^7 + x^6 + x^5 + x^2 + 1 = (x^8 + x^6 + x^4) \cdot (x + 1) + x^4 + x^2 + 1.$$

$$x^8 + x^6 + x^4 = (x^4 + x^2 + 1) \cdot x^4 + 0.$$

$$\text{Por tanto, } \text{mcd}(p(x), p'(x)) = x^4 + x^2 + 1 \neq 1.$$

2. Sea $p(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$. Entonces $p'(x) = x^8 + x^4 + x^2$. Para calcular el máximo común divisor de $p(x)$ y $p'(x)$ empleamos el algoritmo de Euclides.

En este caso, como la única posibilidad para a es que valga uno, no pondremos esa columna.

$p(x)$	$q(x)$
$x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$	$x^8 + x^4 + x^2$
$x^8 + x^4 + x^2$	$x^6 + x^2 + 1$
$x^6 + x^2 + 1$	0

luego $\text{mcd}(p(x), p'(x)) = x^6 + x^2 + 1$. De hecho,

$$p(x) = (x^6 + x^2 + 1)(x^3 + x^2 + 1) \quad p'(x) = (x^6 + x^2 + 1)x^2$$

Si $q(x) = x^6 + x^2 + 1$ se tiene que $q'(x) = 0$. Nótese que $q(x)$ no es irreducible, pues $q(x) = (x^3 + x + 1)^2$.

La factorización de $p(x)$ es $p(x) = (x^3 + x + 1)^2(x^3 + x^2 + 1)$.

3. Sea $p(x) = x^7 + 2x^6 + x^5 + x^4 + x + 2 \in \mathbb{Z}_3[x]$. Su derivada vale $p'(x) = x^6 + 2x^4 + x^3 + 1$. Vamos a calcular $\text{mcd}(p(x), p'(x))$.

a	$p(x)$	$q(x)$
	$x^7 + 2x^6 + x^5 + x^4 + x + 2$	$x^6 + 2x^4 + x^3 + 1$
	$x^6 + 2x^4 + x^3 + 1$	$2x^5 + 2x^4 + x^3$
	$2x^5 + 2x^4 + x^3$	$x^4 + 1$
	$x^4 + 1$	$x^3 + x + 1$
	$x^3 + x + 1$	$2x^2 + 2x + 1$
2	$2x^2 + 2x + 1$	0
	$x^2 + x + 2$	

Es decir, $\text{mcd}(p(x), p'(x)) = x^2 + x + 2$

A partir de esto es fácil ver que la factorización de $p(x)$ es $(x^2 + x + 2)^2(x^3 + 2x + 2)$.

Vemos por tanto, que para encontrar los factores múltiples de un polinomio lo que hay que hacer es calcular el máximo común divisor del polinomio y su derivada.

3.3.4. Factorización de polinomios en $\mathbb{Z}_p[x]$

Ya comentamos la existencia de un algoritmo (algoritmo de Berlekamp) para factorizar polinomios con coeficientes en \mathbb{Z}_p . Pero nosotros aquí, lo único que vamos a hacer es ir probando por los distintos irreducibles para ver si encontramos un divisor de un polinomio.

Supongamos entonces que tenemos un polinomio $q(x) \in \mathbb{Z}_p[x]$ de grado n . Si el polinomio es reducible, entonces tiene un factor irreducible de grado menor o igual que $\frac{n}{2}$.

Comprobamos en primer lugar si tiene o no divisores de grado 1, es decir, comprobamos si tiene raíces. A continuación comprobamos si tiene divisores irreducibles de grado 2, y así sucesivamente.

Ejemplo 3.3.12.

1. Sea $q(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Al ser de grado 3 únicamente hay que comprobar si tiene o no raíces. Puesto que $q(0) = q(1) = 1$ podemos deducir que el polinomio es irreducible. De la misma forma se comprueba que $x^3 + x^2 + 1$ es irreducible.

2. Sea ahora $q(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$. En este caso $q(0) = q(1) = 1$, luego no tiene ningún divisor de grado 1.

Probamos a dividir por $x^2 + x + 1$, que es irreducible de grado 2, y nos queda que $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$. Los dos polinomios que aparecen son irreducibles (pues no tienen raíces).

3. Sea $q(x) = x^7 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$. Entonces:

Evaluamos en $x = 0$ y $x = 1$. En ambos casos nos sale 1, luego $q(x)$ no tiene divisores de grado 1.

Dividimos por $x^2 + x + 1$, y nos queda $q(x) = (x^2 + x + 1)(x^5 + x^4 + x + 1) + x$. Por tanto no tiene divisores de grado 2.

Dividimos por $x^3 + x + 1$ y $x^3 + x^2 + 1$. En el primer caso nos queda $q(x) = (x^3 + x + 1)(x^4 + x^2) + (x^2 + x + 1)$ y en el segundo $q(x) = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1)$.

Puesto que $x^4 + x^3 + x^2 + x + 1$ no tiene divisores de grado 1 y grado 2 (ya que de tenerlos serían también divisores de $q(x)$) deducimos que $x^4 + x^3 + x^2 + x + 1$ es irreducible.

La factorización de $q(x)$ como producto de irreducibles es

$$x^7 + x^4 + x^3 + x + 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1).$$

Como vemos, para factorizar un polinomio en $\mathbb{Z}_p[x]$ es conveniente conocer los polinomios irreducibles mónicos de grado bajo, pues son por los que hemos de efectuar las divisiones. A continuación calcularemos algunos de estos irreducibles.

1. Polinomios irreducibles en $\mathbb{Z}_2[x]$

- ▮ Grado 1. Aquí, los irreducibles son todos, es decir,

$$x \quad x + 1.$$

- ▮ Grado 2. Los no irreducibles son x^2 , $x(x + 1) = x^2 + x$ y $(x + 1)(x + 1) = x^2 + 1$. El único que queda es

$$x^2 + x + 1.$$

- ▮ Grado 3. También aquí los únicos que hay son los que no tienen raíces. Estos son:

$$x^3 + x + 1 \quad x^3 + x^2 + 1.$$

- ▮ Grado 4. Aquí hemos de eliminar todos los que tengan raíces y $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Nos quedan entonces tres polinomios, que son:

$$x^4 + x + 1 \quad x^4 + x^3 + 1 \quad x^4 + x^3 + x^2 + x + 1.$$

- Grado 5. Los reducibles son los que tienen raíces y los dos que toman una factorización de la forma (grado 2) · (grado 3). Estos dos son $(x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1$ y $(x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1$.

Nos quedan entonces 6 polinomios que son:

$$\begin{array}{ccccccc} x^5 + x^2 + 1 & x^5 + x^3 + 1 & x^5 + x^4 + x^3 + x^2 + 1 & x^5 + x^4 + x^3 + x + 1 \\ & x^5 + x^4 + x^2 + x + 1 & & x^5 + x^3 + x^2 + x + 1. \end{array}$$

2. Polinomios mónicos irreducibles en $\mathbb{Z}_3[x]$.

- Grado 1. Al igual que antes, todos son irreducibles. Tenemos por tanto

$$x \quad x + 1 \quad x + 2.$$

- Grado 2. Son aquellos que no tiene raíces. Hay un total de 3, que son:

$$x^2 + 1 \quad x^2 + x + 2 \quad x^2 + 2x + 2.$$

- Grado 3. Son también los que no tienen raíces. En este caso hay 8.

$$\begin{array}{ccccccc} x^3 + 2x + 1 & x^3 + 2x + 2 & x^3 + x^2 + 2 & x^3 + 2x^2 + 1 \\ x^3 + x^2 + x + 2 & x^3 + x^2 + 2x + 1 & x^3 + 2x^2 + x + 1 & x^3 + 2x^2 + 2x + 2. \end{array}$$

- De grado 4 hay 18 polinomios irreducibles.

3. Polinomios mónicos irreducibles en $\mathbb{Z}_5[x]$.

- Grado 1. Tenemos 5 irreducibles:

$$x \quad x + 1 \quad x + 2 \quad x + 3 \quad x + 4.$$

- Grado 2. Los que no tienen raíces son 10.

$$\begin{array}{ccccccc} x^2 + 2 & x^2 + 3 & x^2 + x + 1 & x^2 + x + 2 & x^2 + 2x + 3 \\ x^2 + 2x + 4 & x^2 + 3x + 3 & x^2 + 3x + 4 & x^2 + 4x + 1 & x^2 + 4x + 2. \end{array}$$

- Para grados mayores el número de polinomios es muy grande. Así, de grado 3 la lista tendría 40 polinomios, mientras que la de grado 4 sería de 150.

4. Polinomios mónicos irreducibles en $\mathbb{Z}_7[x]$.

- Grado 1. Como siempre aquí son todos irreducibles.

$$x \quad x + 1 \quad x + 2 \quad x + 3 \quad x + 4 \quad x + 5 \quad x + 6.$$

- Grado 2. Aquí la lista es ya muy grande. Tenemos un total de 21 polinomios.

$$\begin{array}{ccccccccccc} x^2 + 1 & x^2 + 2 & x^2 + 4 & x^2 + x + 3 & x^2 + x + 4 & x^2 + x + 6 & x^2 + 2x + 2 \\ x^2 + 2x + 3 & x^2 + 2x + 5 & x^2 + 3x + 1 & x^2 + 3x + 5 & x^2 + 3x + 6 & x^2 + 4x + 1 & x^2 + 4x + 5 \\ x^2 + 4x + 6 & x^2 + 5x + 2 & x^2 + 5x + 3 & x^2 + 5x + 5 & x^2 + 6x + 3 & x^2 + 6x + 4 & x^2 + 6x + 6. \end{array}$$

- De grado 3 hay un total de 112 polinomios irreducibles.

3.3.5. Factorización de polinomios con coeficientes enteros o racionales.

El lema de Gauss

En este apartado vamos a desarrollar una idea que ya hemos mencionado previamente. La relación entre la factorización de polinomios con coeficientes en \mathbb{Z} y \mathbb{Q} .

El resultado clave es el que da nombre a la sección: el lema de Gauss.

Recordemos que el contenido de un polinomio con coeficientes enteros se definía como el máximo común divisor de sus coeficientes.

Lema 3.3.1 (Lema de Gauss). Sean $q_1(x), q_2(x) \in \mathbb{Z}[x]$ dos polinomios primitivos. Entonces $q_1(x) \cdot q_2(x)$ es primitivo.

Demostración: Supongamos que $q_1(x) \cdot q_2(x)$ no es primitivo. Entonces $c(q_1(x) \cdot q_2(x)) \neq 1$. Sea entonces p un primo que divide a $c(q_1(x) \cdot q_2(x))$.

Supongamos también que $q_1(x) = a_n x^n + \dots + a_1 x + a_0$ y que $q_2(x) = b_m x^m + \dots + b_1 x + b_0$. Puesto que $q_1(x)$ es primitivo, debe existir un coeficiente que no sea múltiplo de p . Supongamos que el primero de ellos es a_k . De la misma forma, sea b_l el primer coeficiente de $q_2(x)$ que no es múltiplo de p . Entonces el coeficiente de grado $k+l$ del polinomio $q_1(x) \cdot q_2(x)$ es

$$a_0 b_{k+l} + \dots + a_{k-1} b_{l+1} + a_k b_l + a_{k+1} b_{l-1} + \dots + a_{k+l} b_0$$

Puesto que a_0, \dots, a_{k-1} son todos múltiplos de p se tiene que $a_0 b_{k+l} + \dots + a_{k-1} b_{l+1}$ es múltiplo de p . Puesto que b_0, \dots, b_{l-1} son múltiplos de p también lo es $a_{k+1} b_{l-1} + \dots + a_{k+l} b_0$, y como el término de grado $k+l$ de $q_1(x) \cdot q_2(x)$ es múltiplo de p deducimos que $a_k b_l$ es múltiplo de p , lo cual no es posible, pues ni a_k ni b_l lo son (recordemos la proposición 2.5.1). ■

Corolario 3.3.2. Sean $p(x), q(x) \in \mathbb{Z}[x]$. Entonces $c(p(x) \cdot q(x)) = c(p(x)) \cdot c(q(x))$.

Demostración: Se tiene que $p(x) = c(p(x)) \cdot p_1(x)$ y $q(x) = c(q(x)) \cdot q_1(x)$, donde $p_1(x)$ y $q_1(x)$ son primitivos. Entonces

$$p(x) \cdot q(x) = [c(p(x)) \cdot p_1(x)] \cdot [c(q(x)) \cdot q_1(x)] = [c(p(x)) \cdot c(q(x))] \cdot p_1(x) \cdot q_1(x)$$

y como $p_1(x) \cdot q_1(x)$ es primitivo deducimos que

$$c(p(x) \cdot q(x)) = c(p(x)) \cdot c(q(x))$$

■

Ejemplo 3.3.13.

- Sean $p(x) = 3x^6 + 5x^5 - 4x^4 + 6x^3 - 10x^2 + 10x - 20$ y $q(x) = 2x^5 + 15x^4 - 12x^3 + 8x^2 - 18x + 12$. Claramente, ambos polinomios son primitivos. Si los multiplicamos nos queda

					3	5	-4	6	-10	10	-20
						2	15	-12	8	-18	12
					36	60	-48	82	-120	120	-240
			-54	-90	72	-108	180	-180	-360		
		24	40	-32	48	-80	80	-160			
	-36	-60	48	-72	120	-120	240				
	45	75	-60	90	-150	150	-300				
6	10	-8	12	-20	20	-40					
6	55	31	-84	104	-234	410	-656	572	-460	-240	-240

es decir,

$$p(x) \cdot q(x) = 6x^{11} + 55x^{10} - 31x^9 - 84x^8 + 104x^7 - 234x^6 + 410x^5 - 656x^4 + 572x^3 - 460x^2 - 240x - 240$$

que también es primitivo.

Si analizamos los coeficientes, vemos que el primer coeficiente de $p(x)$ que no es múltiplo de 2 es el de grado 5 ($5x^5$), mientras que el primero de $q(x)$ que no es de múltiplo de 2 es el de grado 4 ($15x^4$). Al multiplicar los dos polinomios, el primer coeficiente que no es múltiplo de 2 es el de grado 9. Podemos apreciar como todos los sumandos que intervienen en los términos de grado menor o igual que 8 son múltiplos de 2, mientras que en los que intervienen en el de grado 9 todos son múltiplos de 2 salvo uno.

2. El polinomio $2x^2 + 6x - 4$ tiene contenido igual a 2, mientras que el polinomio $12x^2 - 18x + 30$ tiene contenido igual a 6. Su producto, que es $24x^4 - 108x^3 - 96x^2 + 252x - 120$ tiene contenido igual a 12.

Teorema 3.3.3. Sea $p(x) \in \mathbb{Z}[x]$ no constante. Entonces $p(x)$ es irreducible en $\mathbb{Z}[x]$ si, y sólo si, $p(x)$ es primitivo y es irreducible en $\mathbb{Q}[x]$.

Demostración: Sea $p(x) \in \mathbb{Z}[x]$ y supongamos que es irreducible. Claramente es primitivo, pues en caso contrario tendríamos que $c(p(x))|p(x)$.

Si el polinomio fuera reducible en $\mathbb{Q}[x]$ tendríamos una factorización en $\mathbb{Q}[x]$ de la forma $p_1(x) \cdot p_2(x)$. Ahora bien, $p_1(x) = \frac{a}{b}q_1(x)$ y $p_2(x) = \frac{c}{d}q_2(x)$ con $q_1(x), q_2(x) \in \mathbb{Z}[x]$ primitivos. Entonces

$$p(x) = \frac{ac}{bd}q_1(x)q_2(x)$$

Como tanto $p(x)$ como $q_1(x)q_2(x)$ son primitivos, deducimos que $\frac{ac}{bd} = 1$ (o $\frac{ac}{bd} = -1$) lo que nos dice que $p(x) = q_1(x)q_2(x)$ es una factorización en $\mathbb{Z}[x]$, en contra de la hipótesis de que $p(x)$ es irreducible.

Recíprocamente, si $p(x)$ es primitivo e irreducible en $\mathbb{Q}[x]$, si tuviera algún divisor propio en $\mathbb{Z}[x]$ éste no podría ser un polinomio constante, luego sería también un divisor propio en $\mathbb{Q}[x]$. ■

Ejemplo 3.3.14.

1. Sea $p(x) = 6x - 4 \in \mathbb{Z}[x]$. Visto como polinomio en $\mathbb{Q}[x]$ es irreducible, pues es de grado 1. Sin embargo, en $\mathbb{Z}[x]$ no es irreducible, pues $2|(6x - 4)$ y $(3x - 2)|(6x - 4)$.
2. Sea $p(x) = 6x^3 - 19x^2 - 8x + 12$. Podemos ver que este polinomio no es irreducible en $\mathbb{Q}[x]$, pues $x = \frac{2}{3}$ es una raíz, ya que

$$p\left(\frac{2}{3}\right) = 6\left(\frac{2}{3}\right)^3 - 19\left(\frac{2}{3}\right)^2 - 8\frac{2}{3} + 12 = 6\frac{8}{27} - 19\frac{4}{9} - 8\frac{2}{3} + 12 = \frac{16}{9} - \frac{76}{9} - \frac{48}{9} + \frac{108}{9} = 0$$

Dividimos por $x - \frac{2}{3}$

$$\begin{array}{r|rrrr} & 6 & -19 & -8 & 12 \\ \frac{2}{3} & & 4 & -10 & -12 \\ \hline & 6 & -15 & -18 & 0 \end{array}$$

$$\text{luego } p(x) = \left(x - \frac{2}{3}\right)(6x^2 - 15x - 18) = \left[\frac{1}{3}(3x - 2)\right] \cdot [3 \cdot (2x^2 - 5x - 6)] = (3x - 2)(2x^2 - 5x - 6)$$

Vemos como el polinomio es reducible en $\mathbb{Z}[x]$.

Dejamos anteriormente la demostración de la proposición 3.3.3. Recordemos que esta proposición decía que si $p(x)$ es un polinomio primitivo y $\frac{a}{b}$ es una raíz racional de $p(x)$ tal que $\text{mcd}(a, b) = 1$ entonces para cualquier número entero c se tiene que $(bc - a)$ es un divisor de $p(c)$.

Ahora podemos demostrarla. Por ser $\frac{a}{b}$ una raíz racional, se tiene que $p(x) = \left(x - \frac{a}{b}\right) \cdot p_1(x)$. Es fácil ver ahora que el contenido del polinomio $p_1(x)$ vale b (¿por qué?), luego el polinomio $\frac{p_1(x)}{b}$ tiene los coeficientes enteros, y para cualquier número entero c , $\frac{p_1(c)}{b} \in \mathbb{Z}$. Se tiene la siguiente factorización en $\mathbb{Z}[x]$.

$$p(x) = (bx - a) \cdot \frac{p_1(x)}{b}, \text{ luego } p(c) = (bc - a) \cdot \frac{p_1(c)}{b}$$

Es decir, $p(c)$ es múltiplo de $bc - a$.

Criterios de irreducibilidad.

Hemos visto que, salvo constantes, los polinomios irreducibles en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ son los mismos. Vamos a continuación a dar unos criterios que nos van a permitir asegurar que un polinomio primitivo con coeficientes en \mathbb{Z} es irreducible (y por tanto, que un polinomio con coeficientes en \mathbb{Q} es irreducible). Estos criterios **nunca** nos sirven para afirmar que un polinomio es reducible.

Proposición 3.3.7 (Criterio de Eisenstein). *Sea $q(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ primitivo. Supongamos que existe un número primo p tal que $p|a_i : i = 0, 1, \dots, n-1$ y $p^2 \nmid a_0$. Entonces $q(x)$ es irreducible.*

Demostración: Hagamos la demostración por reducción al absurdo. Supongamos entonces que $q(x)$ fuera reducible. Entonces tendríamos una factorización de la forma

$$q(x) = (b_m x^m + \cdots + b_1 x + b_0)(c_k x^k + \cdots + c_1 x + c_0).$$

Puesto que $a_0 = b_0 c_0$, deducimos que $p|b_0 c_0$, luego p divide a uno de los dos coeficientes. Además no puede dividir a los dos, pues en ese caso tendríamos que $p^2|a_0$. Suponemos, por ejemplo, que $p|b_0$ (y por tanto que $p \nmid c_0$).

Supongamos ahora que $p|b_0, p|b_1, \dots, p|b_i$. Vamos a demostrar que $p|b_{i+1}$. Se tiene que

$$a_{i+1} = b_0 c_{i+1} + b_1 c_i + \cdots + b_i c_1 + b_{i+1} c_0.$$

Todos los sumandos, salvo quizá el último son múltiplos de p . También la suma total (a_{i+1}) es múltiplo de p . Por tanto, tenemos que $b_{i+1} c_0$ es múltiplo de p . Como c_0 no lo es, deducimos que b_{i+1} es múltiplo de p .

De esta forma demostramos que todos los coeficientes de $b_m x^m + \cdots + b_1 x + b_0$ son múltiplos de p , lo que implicaría que $a_n = b_m c_k$ sería múltiplo de p , lo cual no es posible. ■

Ejemplo 3.3.15.

1. El polinomio $x^2 + 4x + 4$ satisface todas las hipótesis del criterio de Eisenstein para el primo $p = 2$ salvo la que afirma que $p^2 \nmid a_0$. Vemos que este polinomio es reducible, pues $x^2 + 4x + 4 = (x + 2)^2$.
2. El polinomio $x^2 + 4x + 8$ satisface también todas las hipótesis del criterio de Eisenstein para el primo $p = 2$ salvo la que afirma que $p^2 \nmid a_0$. En este caso el polinomio es irreducible.
3. El polinomio $5x^5 + 6x^4 - 12x^2 + 18x - 24$ satisface las hipótesis del criterio de Eisenstein para $p = 3$. Por tanto es irreducible. Nótese que para $p = 2$ no es posible aplicar el criterio.
4. Para cualquier primo p , los polinomios $x^n + p$ y $x^n - p$ son irreducibles.

Los dos primeros ejemplos nos dicen que si suprimimos una de las hipótesis del criterio de Eisenstein, no podemos afirmar nada sobre el polinomio, pues en el primer caso es reducible y en el segundo es irreducible.

Proposición 3.3.8. [Reducción módulo un primo] *Sea $q(x) \in \mathbb{Z}[x]$, y p un número primo. Denotemos por $\bar{q}(x)$ al polinomio en $\mathbb{Z}_p[x]$ cuyos coeficientes son los de $q(x)$ que se han reducido módulo p . Entonces, si $gr(\bar{q}(x)) = gr(q(x))$ y $\bar{q}(x)$ es irreducible podemos asegurar que $q(x)$ es irreducible.*

Este criterio se suele enunciar diciendo que si $q(x)$ es irreducible en $\mathbb{Z}_p[x]$ entonces $q(x)$ es irreducible en $\mathbb{Z}[x]$.

Demostración: Demostraremos el contrarrecíproco, es decir, si $q(x)$ es reducible en $\mathbb{Z}[x]$ entonces $\bar{q}(x)$ es reducible en $\mathbb{Z}_p[x]$.

Ahora bien, si $q(x)$ es reducible en $\mathbb{Z}[x]$ se tiene que $q(x) = q_1(x) \cdot q_2(x)$, de donde $\bar{q}(x) = \bar{q}_1(x) \cdot \bar{q}_2(x)$ en $\mathbb{Z}_p[x]$. Esta última afirmación es cierta pues si $a_i = b_0 c_i + \cdots + b_i c_0$ en \mathbb{Z} entonces $a_i = b_0 c_i + \cdots + b_i c_0$ en \mathbb{Z}_p para cualquier primo p .

Tenemos por tanto que toda factorización en $\mathbb{Z}[x]$ da lugar a una factorización en $\mathbb{Z}_p[x]$. ■

Aunque no se haya mencionado en la demostración, la hipótesis de que $gr(q(x)) = gr(\bar{q}(x))$ es importante. Analiza en que momento de la demostración es necesaria. En el siguiente ejemplo puedes encontrar alguna ayuda.

En lo que sigue, denotaremos por $q(x)$ tanto al polinomio con coeficientes en \mathbb{Z} como al polinomio con coeficientes en \mathbb{Z}_p .

Ejemplo 3.3.16.

1. Sea $q(x) = 2x^3 - 15x^2 + 19x - 7$. Si reducimos el polinomio módulo 2 nos queda $q(x) = x^2 + x + 1$, que sabemos que es irreducible. Sin embargo, $q(x)$ es reducible, pues $q(x) = (2x - 1)(x^2 - 5x + 7)$.
2. El polinomio $x^5 + 4x^4 - 7x^3 + 12x^2 - 10x + 9$ es irreducible en $\mathbb{Z}[x]$, y por tanto en $\mathbb{Q}[x]$ pues al reducirlo módulo 2 nos queda $x^5 + x^3 + 1$, que es irreducible.
3. Consideramos el polinomio $x^4 - 4x^3 + 3x^2 + 7x - 5$. Si lo reducimos módulo 2 nos queda $x^4 + x^2 + x + 1$ que es reducible, pues $x = 1$ es una raíz. De hecho $x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1)$. Si reducimos módulo 3 nos queda $q(x) = x^4 + 2x^3 + x + 1$. Evaluamos $q(x)$ en los diferentes puntos de \mathbb{Z}_3 y comprobamos que no tiene raíces ($q(0) = 1$, $q(1) = 2$, $q(2) = 2$). Dividimos por los polinomios irreducibles de grado 2, y nos sale:

$$\begin{aligned} x^4 + 2x^3 + x + 1 &= (x^2 + 1)(x^2 + 2x + 2) + 2x + 2 \\ x^4 + 2x^3 + x + 1 &= (x^2 + x + 2)(x^2 + x) + x + 1 \end{aligned}$$

Por tanto $q(x)$ es irreducible en \mathbb{Z}_3 . Deducimos entonces que $x^4 - 4x^3 + 3x^2 + 7x - 5$ es irreducible en $\mathbb{Z}[x]$.

4. El polinomio $q(x) = x^5 + 3x^4 + 3x^3 - 4x + 3$ es reducible en $\mathbb{Z}[x]$ y su factorización como producto de irreducibles es $(x^2 + 2x + 3)(x^3 + x^2 - 2x + 1)$. Si lo reducimos módulo 2 nos queda $q(x) = x^5 + x^4 + x^3 + 1 = (x + 1)^2(x^3 + x^2 + 1)$. Obviamente, al reducir $q(x)$ módulo 2 nos debe quedar un polinomio reducible. Además, la factorización que tenemos en $\mathbb{Z}[x]$ pasa a una factorización en $\mathbb{Z}_2[x]$. Los factores puede ocurrir que sean reducibles módulo 2. En el caso que nos ocupa, uno de los factores $(x^2 + 2x + 3)$ es reducible ($x^2 + 2x + 3 = x^2 + 1 = (x + 1)^2$), mientras que el otro $(x^3 + x^2 - 2x + 1 = x^3 + x^2 + 1)$ es irreducible.
5. Tomamos el polinomio $q(x) = x^4 + 1 \in \mathbb{Z}[x]$.

Este polinomio en $\mathbb{Z}_2[x]$ es reducible. Su factorización es $q(x) = (x + 1)^4$.

En $\mathbb{Z}_3[x]$ es también reducible. Su factorización es $q(x) = (x^2 + x + 2)(x^2 + 2x + 2)$.

En $\mathbb{Z}_5[x]$ es también reducible. Su factorización es $q(x) = (x^2 + 2)(x^2 + 3)$.

En $\mathbb{Z}_7[x]$ es reducible. Su factorización es $q(x) = (x^2 + 3x + 1)(x^2 + 4x + 1)$.

En $\mathbb{Z}_{11}[x]$ es reducible. Su factorización es $q(x) = (x^2 + 3x + 10)(x^2 + 8x + 10)$.

En $\mathbb{Z}_{13}[x]$ es reducible. Su factorización es $q(x) = (x^2 + 5)(x^2 + 8)$.

En $\mathbb{Z}_{17}[x]$ es reducible. Su factorización es $q(x) = (x + 2)(x + 8)(x + 9)(x + 15)$.

En general, para cualquier primo p , el polinomio $q(x) = x^4 + 1$ es reducible en $\mathbb{Z}_p[x]$. Sin embargo, $q(x)$ es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$. Para comprobarlo, podemos calcular su factorización como producto de irreducibles en $\mathbb{R}[x]$, que es $q(x) = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$, y ninguno de ellos tiene sus coeficientes en \mathbb{Q} .

Por tanto, en el caso de que el polinomio $q(x)$ sea reducible en $\mathbb{Z}_p[x]$, no podemos afirmar nada sobre la reducibilidad o irreducibilidad de $q(x)$.

Este método, en principio sólo puede ser aplicado cuando encontramos un primo p donde el polinomio de partida es irreducible en $\mathbb{Z}_p[x]$. Sin embargo, profundizando un poco más en la idea que subyace a este criterio (toda factorización en $\mathbb{Z}[x]$ se mantiene al reducir el polinomio módulo p) podemos afinar algo más a la hora de aplicar el criterio. Antes de explicar como funcionaría veremos algunos ejemplos.

Ejemplo 3.3.17.

1. Sea $q(x) = x^4 - 2x^3 + 3x^2 + x - 1$. Reducimos módulo 2 y factorizamos:

$$x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1)$$

y en principio no podemos deducir nada. Reducimos entonces módulo 3.

$$x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2)$$

y el polinomio resulta ser también reducible.

Ahora bien, si $q(x)$ fuera reducible, la factorización suya se mantendría al reducir $q(x)$ módulo 2. Puesto que en $\mathbb{Z}_2[x]$ se tiene que $q(x)$ es producto de un polinomio de grado 1 por uno de grado 3 deducimos que si $q(x)$ es reducible, entonces se factoriza como un polinomio de grado 1 por uno de grado 3.

Pero también la factorización de $q(x)$ se mantendría al reducirlo módulo 3. Sin embargo, en $\mathbb{Z}_3[x]$, el polinomio $q(x)$ no tiene ninguna raíz, luego no podemos tener una factorización de $q(x)$ de la forma (grado 1)·(grado 3).

Deducimos entonces que $q(x)$ es irreducible.

En este caso se dice que las factorizaciones de $q(x)$ módulo 2 y módulo 3 son incompatibles.

2. En el ejemplo precedente, una vez vista la factorización en $\mathbb{Z}_2[x]$ bastaría comprobar que no tiene raíces en \mathbb{Q} . Puesto que $q(1) = 2$ y $q(-1) = 4$ podemos deducir que $q(x)$ es irreducible.
3. Sea $q(x) = x^4 + 4x^3 + 6x^2 + x - 4$. Si reducimos módulo 2 obtenemos:

$$x^4 + x = x(x + 1)(x^2 + x + 1)$$

mientras que al reducir módulo 3 nos da

$$x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2)$$

En este caso tenemos dos factorizaciones distintas, sin embargo no son incompatibles, pues en ambos casos tenemos una posible factorización (grado 2)·(grado 2).

De hecho, este polinomio es reducible, pues $x^4 + 4x^3 + 6x^2 + x - 4 = (x^2 + 3x + 4)(x^2 + x - 1)$.

Definición 51. Sea $q(x) \in \mathbb{Z}[x]$, y p un número primo tal que al reducir $q(x)$ módulo p no disminuye el grado. Definimos el conjunto D_p (o $D_p(q(x))$) como el conjunto formado por los grados de los divisores propios de $q(x)$ en $\mathbb{Z}_p[x]$.

Si p_1, \dots, p_k son números primos, se define el conjunto D_{p_1, \dots, p_k} como

$$D_{p_1, \dots, p_k} = D_{p_1} \cap \dots \cap D_{p_k}$$

Ejemplo 3.3.18.

1. Si $q(x) = x^4 - 2x^3 + 3x^2 + x - 1$ entonces $D_2 = \{1, 3\}$, pues sus divisores son $x + 1$ y $x^3 + x^2 + 1$, que tienen grados 1 y 3 respectivamente. Por otra parte, $D_3 = \{2\}$, pues cualquier divisor suyo tiene grado 2.

Por tanto se tiene que $D_{2,3} = \emptyset$.

2. Si $q(x) = x^4 + 4x^3 + 6x^2 + x - 4$ entonces $D_2 = \{1, 2, 3\}$.

Son divisores de grado 1, x y $x + 1$.

Son divisores de grado 2, $x(x + 1)$ y $x^2 + x + 1$.

Son divisores de grado 3, $x(x^2 + x + 1)$ y $(x + 1)(x^2 + x + 1)$.

Mientras que $D_3 = \{2\}$. Por tanto $D_{2,3} = \{2\}$.

Claramente se tiene que $q(x)$ es irreducible en $\mathbb{Z}_p[x]$ si, y sólo si, $D_p = \emptyset$.

Por otra parte, se tiene que si existen primos p_1, \dots, p_k tales que $D_{p_1, \dots, p_k} = \emptyset$ entonces $q(x)$ es irreducible.

Sin embargo, aunque esto mejora a la proposición 3.3.8, en algunos casos puede no servirnos para deducir si un polinomio es reducible o irreducible. Por ejemplo, hemos visto que $x^4 + 1$ es irreducible, y sin embargo, $2 \in D_{2,3,5,7,11,13,17}$. De hecho, para cualquier primo p se tiene que $2 \in D_p(x^4 + 1)$.

3.4. Anillos cocientes de polinomios. Cuerpos finitos

En los capítulos anteriores, dado un número natural $n \geq 2$, construimos el conjunto \mathbb{Z}_n , y después definimos su aritmética.

Ahora, sustituimos \mathbb{Z} por $K[x]$, con K un cuerpo. Si $m(x) \in K[x]$ vamos a definir el conjunto $K[x]_{m(x)}$. Para esto, necesitamos definir la relación de congruencia entre polinomios, de forma análoga a como se hizo con números enteros.

Definición 52. Sea K un cuerpo y $a(x), b(x), m(x) \in K[x]$. Se dice que $a(x)$ es congruente con $b(x)$ módulo $m(x)$, y se escribe $a(x) \equiv b(x) \pmod{m(x)}$ si $m(x) \mid (b(x) - a(x))$. Es decir:

$$a(x) \equiv b(x) \pmod{m(x)} \text{ si existe } c(x) \in K[x] \text{ tal que } b(x) - a(x) = c(x)m(x).$$

Nótese que la relación de congruencia módulo 0 es la relación de igualdad ($a(x) \equiv b(x) \pmod{0}$) si, y sólo si, $a(x) = b(x)$, mientras que si $\lambda \in K^*$ entonces $a(x) \equiv b(x) \pmod{\lambda}$ cualesquiera que sean $a(x)$ y $b(x)$. Por tanto, nos centraremos en congruencias módulo $m(x)$ con $m(x)$ un polinomio de grado mayor o igual que 1.

Además, se tiene que $a(x) \equiv b(x) \pmod{m(x)}$ si, y sólo si, $a(x) \equiv b(x) \pmod{\lambda \cdot m(x)}$, donde $\lambda \in K^*$. Por tanto, al hablar de congruencias módulo $m(x)$ podemos suponer que $m(x)$ es un polinomio mónico.

Ejemplo 3.4.1. Sea $m(x) = x^2 + 2 \in \mathbb{Z}_3[x]$. Entonces:

$$x^4 + 2x^3 + x^2 + x + 2 \equiv 2x^4 + x^3 + 2x^2 + 2x \pmod{x^2 + 2}$$

$$\text{pues } (2x^4 + x^3 + 2x^2 + 2x) - (x^4 + 2x^3 + x^2 + x + 2) = (x^2 + 2)(x^2 + 2x + 2).$$

$$x^4 + x^3 + 2x^2 + 1 \not\equiv x^3 + x + 2 \pmod{x^2 + 2}$$

$$\text{ya que } (x^3 + x + 2) - (x^4 + x^3 + 2x^2 + 1) = 2x^2(x^2 + 2) + (x + 1).$$

Proposición 3.4.1. Sea $m(x) \in K[x]$. Entonces la relación de congruencia módulo $m(x)$ es una relación de equivalencia.

La demostración es igual a la que se hizo para congruencias en \mathbb{Z} .

Para cada $m(x) \in K[x]$ vamos a denotar por $K[x]_{m(x)}$ al conjunto cociente de $K[x]$ por la relación de congruencia módulo $m(x)$. A la clase de equivalencia de un polinomio $a(x)$ la denotaremos inicialmente por $[a(x)]_{m(x)}$, o simplemente $[a(x)]$.

Al igual que en el caso de los números enteros, se tiene que $a(x) \equiv b(x) \pmod{m(x)}$ si, y sólo si, $a(x) \pmod{m(x)} = b(x) \pmod{m(x)}$ (es decir, dan el mismo resto al dividir por $m(x)$). A partir de aquí puede verse que el conjunto $K[x]_{m(x)}$ está en biyección con los polinomios de $K[x]$ de grado menor que el de $m(x)$, pues hay tantos elementos como posibles restos de la división por $m(x)$.

Ejemplo 3.4.2.

1. Vamos a calcular los elementos del conjunto $\mathbb{Z}_2[x]_{(x^2+1)}$.

Sea $p(x) \in \mathbb{Z}_2[x]$. Si dividimos $p(x)$ entre $x^2 + 1$, sólo tenemos cuatro posibles restos, que son 0, 1, x y $x + 1$, ya que el resto es de grado menor que 2. Tenemos entonces que

$$\mathbb{Z}_2[x]_{x^2+1} = \{[0], [1], [x], [x+1]\}.$$

En la clase de equivalencia $[0]$ están todos los polinomios que dan resto cero al dividir por $x^2 + 1$, es decir, todos los múltiplos de $x^2 + 1$, por ejemplo, $0, x^2 + 1, x^3 + x, x^4 + 1$, etc.; en la clase $[1]$ están los polinomios que al dividir por $x^2 + 1$ dan resto 1, como por ejemplo, $1, x^2, x^3 + x + 1, x^4$, etc.

En resumen, se tiene:

$$\begin{aligned} [0] &= \{0, x^2 + 1, x^3 + x, x^3 + x^2 + x + 1, x^4 + x^2, x^4 + 1, x^4 + x^3 + x^2 + x, x^4 + x^3 + x + 1, \dots\}. \\ [1] &= \{1, x^2, x^3 + x + 1, x^3 + x^2 + x, x^4 + x^2 + 1, x^4, x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + x, \dots\}. \\ [x] &= \{x, x^2 + x + 1, x^3, x^3 + x^2 + 1, x^4 + x^2 + x, x^4 + x + 1, x^4 + x^3 + x^2, x^4 + x^3 + 1, \dots\}. \\ [x+1] &= \{x+1, x^2 + x, x^3 + 1, x^3 + x^2, x^4 + x^2 + x + 1, x^4 + x, x^4 + x^3 + x^2 + 1, x^4 + x^3, \dots\}. \end{aligned}$$

O si queremos,

$$\begin{aligned} [0] &= (x^2 + 1)\mathbb{Z}_2[x]; & [1] &= 1 + (x^2 + 1)\mathbb{Z}_2[x]; \\ [x] &= x + (x^2 + 1)\mathbb{Z}_2[x]; & [x+1] &= x + 1 + (x^2 + 1)\mathbb{Z}_2[x]. \end{aligned}$$

Y por ejemplo, se tiene que $x^8 + x^7 + x^6 + x + 1 \in [1]$, ya que

$$x^8 + x^7 + x^6 + x + 1 = 1 + (x^2 + 1) \cdot (x^6 + x^5 + x^3 + x).$$

2. El conjunto $\mathbb{Z}_2[x]_{x^2+x+1}$ tiene también cuatro elementos, que son $[0], [1], [x]$ y $[x+1]$. Sin embargo, aunque se representen igual que los de $\mathbb{Z}_2[x]_{x^2+1}$, los conjuntos $\mathbb{Z}_2[x]_{x^2+x+1}$ y $\mathbb{Z}_2[x]_{x^2+1}$ son distintos, pues en cada uno $[0], [1], [x]$ y $[x+1]$ representa cosas diferentes. Veámoslo.

$$\begin{aligned} [0] &= \{0, x^2 + x + 1, x^3 + x^2 + x, x^3 + 1, x^4 + x^3 + x^2, x^4 + x^3 + x + 1, x^4 + x, x^4 + x^2 + 1, \dots\}. \\ [1] &= \{1, x^2 + x, x^3 + x^2 + x + 1, x^3, x^4 + x^3 + x^2 + 1, x^4 + x^3 + x, x^4 + x + 1, x^4 + x^2, \dots\}. \\ [x] &= \{0, x^2 + 1, x^3 + x^2, x^3 + x + 1, x^4 + x^3 + x^2 + x, x^4 + x^3 + 1, x^4, x^4 + x^2 + x + 1, \dots\}. \\ [x+1] &= \{0, x^2, x^3 + x^2 + 1, x^3 + x, x^4 + x^3 + x^2 + x + 1, x^4 + x^3, x^4 + 1, x^4 + x^2 + x, \dots\}. \end{aligned}$$

Y vemos como, por ejemplo, en el primer caso, es decir, $\mathbb{Z}_2[x]_{x^2+1}$ se tiene que $x^3 \in [x]$ (o $[x^3] = [x]$), mientras que en el segundo caso, es decir, $\mathbb{Z}_2[x]_{x^2+x+1}$ se tiene que $x^3 \in [1]$.

3. El conjunto $\mathbb{Z}_2[x]_{x^3+x^2+x+1}$ tiene ocho elementos, mientras que $\mathbb{Z}_3[x]_{x^2+1}$ tiene nueve. Determinálos en ambos casos.

Lema 3.4.1. Sean $a(x), b(x), c(x), d(x), m(x) \in K[x]$. Entonces:

1. $\left. \begin{aligned} a(x) &\equiv c(x) \pmod{m(x)} \\ b(x) &\equiv d(x) \pmod{m(x)} \end{aligned} \right\} \implies a(x) + b(x) \equiv c(x) + d(x) \pmod{m(x)}.$
2. $\left. \begin{aligned} a(x) &\equiv c(x) \pmod{m(x)} \\ b(x) &\equiv d(x) \pmod{m(x)} \end{aligned} \right\} \implies a(x)b(x) \equiv c(x)d(x) \pmod{m(x)}.$

Y con este lema podemos ya definir las operaciones suma y producto

Definición 53. Sean $a(x), b(x) \in K[x]$ y $m(x) \in K[x]$ mónico y no constante. Se definen en $K[x]_{m(x)}$ las operaciones:

$$[a(x)] + [b(x)] = [a(x) + b(x)], \quad [a(x)][b(x)] = [a(x)b(x)].$$

Como era de esperar, la definición hecha no depende de los representantes elegidos.

Ejemplo 3.4.3.

1. Supongamos que estamos trabajando en $\mathbb{Z}_3[x]_{x^2+1}$.

$$[x+2] + [x+1] = [2x].$$

$$[x+2][x+1] = [x^2+2] = [1].$$

Puesto que $[x+2] = [x^2+x]$ y $[x+1] = [2x^2+x]$ podíamos haber efectuado las operaciones anteriores

$$[x^2+x] + [2x^2+x] = [3x^2+2x] = [2x].$$

$$[x^2+x][2x^2+x] = [2x^4+x^2] = [1], \text{ ya que } 2x^4+x^2 = (x^2+1)(2x^2+2) + 1.$$

Y los resultados coinciden, como no podía ser de otra forma.

2. Vamos a fijarnos ahora en las clases de equivalencia que hemos obtenido en el ejemplo 3.4.2. En ese ejemplo, calculamos las clases de equivalencia que determinaban el conjunto $\mathbb{Z}_2[x]_{x^2+1}$ y las que determinaban el conjunto $\mathbb{Z}_2[x]_{x^2+x+1}$.

Vamos a sumar un elemento cualquiera de $[1]$ con un elemento cualquiera de $[x]$. El resultado va a ser un elemento de $[x+1]$. Lo vamos a hacer cuatro veces.

▮ Primero lo vamos a hacer con clases de $\mathbb{Z}_2[x]_{x^2+1}$.

$$\begin{array}{ll} 1+x = x+1 \in [x+1] & (x^3+x^2+x) + (x^2+x+1) = x^3+1 \in [x+1] \\ x^2+(x^4+x^3+x^2) = x^4+x^3 \in [x+1] & (x^4+x^3+x) + (x^4+x^3+x^2) = x^2+x \in [x+1] \end{array} \quad .$$

Y así para cualesquiera dos polinomios que tomemos, el primero perteneciente a $[1]$ y el segundo a $[x]$.

▮ Ahora lo hacemos en $\mathbb{Z}_2[x]_{x^2+x+1}$.

$$\begin{array}{ll} (x^2+x) + (x^2+1) = x+1 \in [x+1] & x^3+(x^4+x^3+1) = x^4+1 \in [x+1] \\ (x^4+x^3+x) + (x^3+x+1) = x^4+1 \in [x+1] & (x^4+x^2) + x^4 = x^2 \in [x+1] \end{array} \quad .$$

De ahora en adelante, si $a \in K \subseteq K[x]$, denotaremos por a a la clase de equivalencia $[a] \in K[x]_{m(x)}$, mientras que denotaremos por α a la clase de equivalencia $[x]$ (aunque es también frecuente representar por x a $[x]$).

Nótese que siguiendo esta notación, dado $a_k x^k + \dots + a_1 x + a_0 \in K[x]$ el elemento $[a_k x^k + \dots + a_1 x + a_0]$ se representa como $a_k \alpha^k + \dots + a_1 \alpha + a_0$. Dicho de otra forma, $[p(x)]$ se representa como $p(\alpha)$.

Nótese también que con esta notación se verifica que $m(\alpha) = 0$, pues $m(\alpha) = [m(x)] = [0]$. Además, esta condición es suficiente para realizar las operaciones en $K[x]_{m(x)}$

$$K[x]_{m(x)} = \{p(\alpha) : p(x) \in K[x]; m(\alpha) = 0\}.$$

Al igual que ocurría con los conjuntos \mathbb{Z}_m , en los conjuntos que hemos construido, $K[x]_{m(x)}$, también tenemos definidas las operaciones suma y producto. El lema 3.4.1 nos asegura que estas definiciones son correctas.

Ejemplo 3.4.4.

1. En el conjunto $\mathbb{Z}_2[x]_{x^3+x+1}$ vamos a multiplicar $[x^2+x+1]$ y $[x^2+1]$. Podemos proceder de dos formas:

a) Multiplicamos los dos polinomios:

$$[x^2+x+1][x^2+1] = [x^4+x^3+x+1].$$

$$\text{Dividimos } x^4+x^3+x+1 \text{ entre } x^3+x+1. \quad x^4+x^3+x+1 = (x^3+x+1)(x+1) + x^2+x.$$

$$\text{Por tanto } [x^2+x+1][x^2+1] = [x^2+x].$$

b) $(\alpha^2 + \alpha + 1)(\alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha + 1.$

Puesto que $\alpha^3 + \alpha + 1 = 0$ deducimos que $\alpha^3 = \alpha + 1$, luego $\alpha^4 = \alpha^2 + \alpha$. Por tanto

$$(\alpha^2 + \alpha + 1)(\alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha + 1 = (\alpha^2 + \alpha) + (\alpha + 1) + \alpha + 1 = \alpha^2 + \alpha.$$

En los dos casos se obtiene el mismo resultado.

2. $\mathbb{Z}_2[x]_{x^2+1} = \{0, 1, \alpha, \alpha + 1 : \alpha^2 + 1 = 0\}$, o si preferimos:

$$\mathbb{Z}_2[x]_{x^2+1} = \{0, 1, \alpha, \alpha + 1 : \alpha^2 = 1\}.$$

Proposición 3.4.2. Sea $m(x) \in k[x]$ mónico y no constante. Las operaciones suma y producto en $K[x]_{m(x)}$ verifican las siguientes propiedades:

i) $p(\alpha) + (q(\alpha) + r(\alpha)) = (p(\alpha) + q(\alpha)) + r(\alpha)$

ii) $p(\alpha) + q(\alpha) = q(\alpha) + p(\alpha)$

iii) $p(\alpha) + 0 = p(\alpha)$

iv) Para cada $p(\alpha) \in K[x]_{m(x)}$ existe $q(\alpha) \in K[x]_{m(x)}$ tal que $p(\alpha) + q(\alpha) = 0$.

v) $p(\alpha)(q(\alpha)r(\alpha)) = (p(\alpha)q(\alpha))r(\alpha)$

vi) $p(\alpha)q(\alpha) = q(\alpha)p(\alpha)$

vii) $p(\alpha)1 = p(\alpha)$

viii) $p(\alpha)(q(\alpha) + r(\alpha)) = p(\alpha)q(\alpha) + p(\alpha)r(\alpha)$

Estas propiedades nos dicen que $K[x]_{m(x)}$ es un anillo conmutativo.

Ejemplo 3.4.5.

1. Consideramos el anillo $\mathbb{Z}_2[x]_{x^3+1}$. Vamos a escribir las tablas de sumar y multiplicar de dicho anillo. Antes de ello, enumeramos sus elementos

$$\mathbb{Z}_2[x]_{x^3+1} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

+	0	1	α	$\alpha + 1$	α^2	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$
0	0	1	α	$\alpha + 1$	α^2	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$
1	1	0	$\alpha + 1$	α	$\alpha^2 + 1$	α^2	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$
α	α	$\alpha + 1$	0	1	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	α^2	$\alpha^2 + 1$
$\alpha + 1$	$\alpha + 1$	α	1	0	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + 1$	α^2
α^2	α^2	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	0	1	α	$\alpha + 1$
$\alpha^2 + 1$	$\alpha^2 + 1$	α^2	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	1	0	$\alpha + 1$	α
$\alpha^2 + \alpha$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	α^2	$\alpha^2 + 1$	α	$\alpha + 1$	0	1
$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + 1$	α^2	$\alpha + 1$	α	1	0

Para realizar la tabla del producto tenemos en cuenta que $\alpha^3 + 1 = 0$, es decir, $\alpha^3 = 1$.

.	0	1	α	$\alpha + 1$	α^2	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha + 1$	α^2	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$
α	0	α	α^2	$\alpha^2 + \alpha$	1	$\alpha + 1$	$\alpha^2 + 1$	$\alpha^2 + \alpha + 1$
$\alpha + 1$	0	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + 1$	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha + 1$	0
α^2	0	α^2	1	$\alpha^2 + 1$	α	$\alpha^2 + \alpha$	$\alpha + 1$	$\alpha^2 + \alpha + 1$
$\alpha^2 + 1$	0	$\alpha^2 + 1$	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha$	$\alpha + 1$	$\alpha^2 + 1$	0
$\alpha^2 + \alpha$	0	$\alpha^2 + \alpha$	$\alpha^2 + 1$	$\alpha + 1$	$\alpha + 1$	$\alpha^2 + 1$	$\alpha^2 + \alpha$	0
$\alpha^2 + \alpha + 1$	0	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha + 1$	0	$\alpha^2 + \alpha + 1$	0	0	$\alpha^2 + \alpha + 1$

Donde algunas de las celdas se han completado como sigue:

$$\alpha \cdot \alpha^2 = \alpha^3 = 1$$

$$(\alpha^2 + 1)(\alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha^2 + \alpha + 1 = \alpha + 1 + \alpha^2 + \alpha^2 + \alpha + 1 = 0$$

Y se ha tenido en cuenta que $\alpha^4 = \alpha^3 \cdot \alpha = \alpha$.

$$(\alpha^2 + 1)(\alpha^2 + 1) = \alpha^4 + 2\alpha^2 + 1 = \alpha + 1.$$

2. Vamos a dar ahora la tabla de multiplicar de $\mathbb{Z}_3[x]_{x^2+1}$. Los elementos son ahora

$$\mathbb{Z}_3[x]_{x^2+1} = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$$

\cdot	0	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
2	0	2	1	2α	$2\alpha + 2$	$2\alpha + 1$	α	$\alpha + 2$	$\alpha + 1$
α	0	α	2α	2	$\alpha + 2$	$2\alpha + 2$	1	$\alpha + 1$	$2\alpha + 1$
$\alpha + 1$	0	$\alpha + 1$	$2\alpha + 2$	$\alpha + 2$	2α	1	$2\alpha + 1$	2	α
$\alpha + 2$	0	$\alpha + 2$	$2\alpha + 1$	$2\alpha + 2$	1	α	$\alpha + 1$	2α	2
2α	0	2α	α	1	$2\alpha + 1$	$\alpha + 1$	2	$2\alpha + 2$	$\alpha + 2$
$2\alpha + 1$	0	$2\alpha + 1$	$\alpha + 2$	$\alpha + 1$	2	2α	$2\alpha + 2$	α	1
$2\alpha + 2$	0	$2\alpha + 2$	$\alpha + 1$	$2\alpha + 1$	α	2	$\alpha + 2$	1	2α

Definición 54. Sea A un anillo conmutativo.

- ▮ Se dice que $a \in A$ es una unidad si existe $b \in A$ tal que $ab = 1$. En tal caso, se dice que b es el inverso de a , y escribiremos $b = a^{-1}$.
- ▮ Se dice que $a \in A$ es un divisor de cero si existe $b \in A$, $b \neq 0$ tal que $ab = 0$.

Un anillo conmutativo en el que 0 es el único divisor de cero se llama dominio de integridad.

Un anillo conmutativo en el que todo elemento no nulo es una unidad es un cuerpo.

Ejemplo 3.4.6.

1. En cualquier anillo, 1 es una unidad, pues $1 \cdot 1 = 1$, mientras que 0 es un divisor de cero, pues $0 \cdot 1 = 0$.
2. En $\mathbb{Z}_2[x]_{x^3+1}$ son divisores de cero:

$$0 \quad \alpha + 1 \quad \alpha^2 + 1 \quad \alpha^2 + \alpha \quad \alpha^2 + \alpha + 1$$

mientras que son unidades:

$$1 \quad \alpha \quad \alpha^2$$

como puede comprobarse a partir del ejemplo anterior.

3. En $\mathbb{Z}_3[x]_{x^2+1}$, el único divisor de cero es 0. Todos los demás elementos son unidades.
4. En \mathbb{Z} , las unidades son 1 y -1 . El único divisor de cero es 0.
5. Todo cuerpo es un dominio de integridad. El recíproco no es cierto, pues \mathbb{Z} es un dominio de integridad pero no es un cuerpo.

Proposición 3.4.3. Sea K un cuerpo, $m(x) \in K[x]$ no constante y $p(\alpha) \in K[x]_{m(x)}$. Entonces:

- ▮ $p(\alpha)$ es una unidad si, y sólo si, $\text{mcd}(p(x), m(x)) = 1$.
- ▮ $p(\alpha)$ es un divisor de cero si, y sólo si, $\text{mcd}(p(x), m(x)) \neq 1$.

Demostración: La demostración de la primera parte es análoga a la demostración de la proposición 2.6.2

En cuanto a la segunda, si $p(\alpha)$ es un divisor de cero, entonces $p(\alpha)$ no es una unidad (¿por qué?), luego $\text{mcd}(p(x), m(x)) \neq 1$.

Recíprocamente, si $\text{mcd}(p(x), m(x)) \neq 1$, consideramos $q(x) = \frac{m(x)}{d(x)}$ donde $d(x) = \text{mcd}(p(x), m(x))$. Entonces $\text{gr}(q(x)) < \text{gr}(m(x))$, lo que implica que $q(\alpha) \neq 0$, y puesto que $p(x)q(x)$ es múltiplo de $m(x)$ ya que

$$p(x)q(x) = p(x) \frac{m(x)}{d(x)} = \frac{p(x)}{d(x)} m(x)$$

se verifica que $p(\alpha)q(\alpha) = 0$. ■

Ejemplo 3.4.7. En $\mathbb{Z}_2[x]$ se verifica que $\text{mcd}(x^2 + 1, x^3 + 1) = x + 1$. Por tanto, $\alpha^2 + 1$ es un divisor de cero en $\mathbb{Z}_2[x]_{x^3+1}$. Además, para encontrar un elemento que al multiplicarlo por él nos de cero, calculamos $\frac{x^3+1}{x+1}$. Ese cociente vale $x^2 + x + 1$. Deducimos entonces que $(\alpha^2 + 1)(\alpha^2 + \alpha + 1) = 0$, como podemos ver en el ejemplo anterior.

A partir de la proposición anterior se deduce fácilmente que si $m(x)$ es un polinomio irreducible en $K[x]$, entonces $K[x]_{m(x)}$ es un cuerpo. Si $m(x)$ es un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$ entonces $\mathbb{Z}_p[x]_{m(x)}$ es un cuerpo con p^n elementos.

Por otra parte, si K es un cuerpo con un número finito de elementos, entonces su característica es un número primo p (la característica de un anillo A se define como el menor número natural m tal que $1 + 1 + \dots + 1$ (m veces) $+ 1 = 0$, si dicho número existe). En tal caso se tiene que $\mathbb{Z}_p \subseteq K$. Utilizando resultados de álgebra lineal se tiene que existe un número natural n tal que K tiene p^n elementos.

Es decir, por una parte hemos visto que el número de elementos de un cuerpo finito es una potencia de un primo. Por otra parte, hemos visto como, dado un número primo p y un número natural n podemos construir un cuerpo con p^n elementos. Basta encontrar un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$. Hay un teorema que nos asegura la existencia de polinomios irreducibles de cualquier grado en $\mathbb{Z}_p[x]$.

La existencia de varios polinomios irreducibles de un mismo grado en $\mathbb{Z}_p[x]$ daría lugar, en principio, a distintos cuerpos con p^n elementos. Sin embargo, todos los cuerpos con el mismo cardinal son isomorfos, en el sentido que vamos a explicar a continuación.

Ejemplo 3.4.8.

1. Hemos visto que $\mathbb{Z}_3[x]_{x^2+1}$ es un cuerpo con nueve elementos, cuya tabla del producto calculamos en el ejemplo 3.4.5. Puesto que $x^2 + x + 2$ es también un polinomio irreducible en $\mathbb{Z}_3[x]$ tenemos que $\mathbb{Z}_3[x]_{x^2+x+2}$ es también un cuerpo con nueve elementos. Si llamamos β al elemento $[x]$, entonces la tabla del producto de este cuerpo es:

$(\mathbb{Z}_3[x]_{x^2+x+2}, \cdot)$	0	1	2	β	$\beta + 1$	$\beta + 2$	2β	$2\beta + 1$	$2\beta + 2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	β	$\beta + 1$	$\beta + 2$	2β	$2\beta + 1$	$2\beta + 2$
2	0	2	1	2β	$2\beta + 2$	$2\beta + 1$	β	$\beta + 2$	$\beta + 1$
β	0	β	2β	$2\beta + 1$	1	$\beta + 1$	$\beta + 2$	$2\beta + 2$	2
$\beta + 1$	0	$\beta + 1$	$2\beta + 2$	1	$\beta + 2$	2β	2	β	$2\beta + 1$
$\beta + 2$	0	$\beta + 2$	$2\beta + 1$	$\beta + 1$	2β	2	$2\beta + 2$	1	β
2β	0	2β	β	$\beta + 2$	2	$2\beta + 2$	$2\beta + 1$	$\beta + 1$	1
$2\beta + 1$	0	$2\beta + 1$	$\beta + 2$	$2\beta + 2$	β	1	$\beta + 1$	2	2β
$2\beta + 2$	0	$2\beta + 2$	$\beta + 1$	2	$2\beta + 1$	β	1	2β	$\beta + 2$

donde se ha usado que $\beta^2 = 2\beta + 1$, relación que se deduce de $\beta^2 + \beta + 2 = 0$ (es decir, $m(\beta) = 0$).

Si ahora hacemos el cambio $\alpha = \beta + 2$, es decir, $\beta = \alpha + 1$, la tabla nos quedaría

$(\mathbb{Z}_3[x]_{x^2+x+2}, \cdot)$	0	1	2	$\alpha + 1$	$\alpha + 2$	α	$2\alpha + 2$	2α	$2\alpha + 1$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\alpha + 1$	$\alpha + 2$	α	$2\alpha + 2$	2α	$2\alpha + 1$
2	0	2	1	$2\alpha + 2$	$2\alpha + 1$	2α	$\alpha + 1$	α	$\alpha + 2$
$\alpha + 1$	0	$\alpha + 1$	$2\alpha + 2$	2α	1	$\alpha + 2$	α	$2\alpha + 1$	2
$\alpha + 2$	0	$\alpha + 2$	$2\alpha + 1$	1	α	$2\alpha + 2$	2	$\alpha + 1$	2α
α	0	α	2α	$\alpha + 2$	$2\alpha + 2$	2	$2\alpha + 1$	1	$\alpha + 1$
$2\alpha + 2$	0	$2\alpha + 2$	$\alpha + 1$	α	2	$2\alpha + 1$	2α	$\alpha + 2$	1
2α	0	2α	α	$2\alpha + 1$	$\alpha + 1$	1	$\alpha + 2$	2	$2\alpha + 2$
$2\alpha + 1$	0	$2\alpha + 1$	$\alpha + 2$	2	2α	$\alpha + 1$	1	$2\alpha + 2$	α

Si comparamos esta tabla con la que obtuvimos para $\mathbb{Z}_3[x]_{x^2+1}$ vemos que es exactamente la misma (salvo el orden de las filas y columnas). Vemos entonces que los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ son iguales, o más precisamente, son isomorfos.

De hecho, lo único que diferencia a los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ es, aparte del camino para obtenerlos, el nombre que se le ha dado a los elementos. Lo que en un cuerpo se llama α en el otro se llama $\beta + 2$. Una vez hecha la correcta correspondencia entre los elementos de uno y del otro, se opera de igual forma en un caso y en el otro.

Nota: Dados dos cuerpos K y K' , se dice que son isomorfos si existe una aplicación $f : K \rightarrow K'$ satisfaciendo:

- a) f preserva la suma, es decir, $f(a + b) = f(a) + f(b)$.
- b) f preserva el producto, es decir, $f(ab) = f(a)f(b)$.
- c) f es biyectiva.

f es lo que se llama un isomorfismo de cuerpos.

En el caso de $K = \mathbb{Z}_3[x]_{x^2+x+2}$ y $K' = \mathbb{Z}_3[x]_{x^2+1}$, la aplicación $f : K \rightarrow K'$ dada por

$$0 \mapsto 0 \quad 1 \mapsto 1 \quad 2 \mapsto 2 \quad \beta \mapsto \alpha + 1 \quad \beta + 1 \mapsto \alpha + 2$$

$$\beta + 2 \mapsto \alpha \quad 2\beta \mapsto 2\alpha + 2 \quad 2\beta + 1 \mapsto 2\alpha \quad 2\beta + 2 \mapsto 2\alpha + 1$$

es un isomorfismo de cuerpos. Obviamente, este isomorfismo queda totalmente determinado por $\beta \mapsto \alpha + 1$.

2. Nos situamos en el cuerpo de los números reales. Entonces el polinomio $x^2 + 1$ es irreducible, luego $\mathbb{R}[x]_{x^2+1}$ es un cuerpo. Si llamamos i al elemento $[x]$, entonces se tiene que los elementos de $\mathbb{R}[x]_{x^2+1}$ son de la forma $a + bi$, donde $a, b \in \mathbb{R}$. Además, $i^2 + 1 = 0$, es decir, $i^2 = -1$.

Por tanto,

$$\mathbb{R}[x]_{x^2+1} = \{a + bi : a, b \in \mathbb{R}; i^2 = -1\}$$

luego el cuerpo obtenido resulta ser igual (o isomorfo) a \mathbb{C} .

Dado p es un número primo y n es un número natural no nulo, denotaremos como \mathbb{F}_{p^n} al único cuerpo que existe con p^n elementos. Así, por ejemplo, $\mathbb{F}_4 = \mathbb{Z}_2[x]_{x^2+x+1}$ y $\mathbb{F}_9 = \mathbb{Z}_3[x]_{x^2+1}$. Obviamente, $\mathbb{F}_p = \mathbb{Z}_p$ para cualquier primo p .

3.5. Sistemas de congruencias de polinomios

Al igual que se hizo con los números enteros, nos planteamos encontrar todos los polinomios $p(x) \in K[x]$ que verifican la relación

$$a(x)p(x) \equiv b(x) \pmod{m(x)}$$

con $a(x), b(x), m(x) \in K[x]$.

Un polinomio $q(x) \in K[x]$ para el que se verifique que $a(x)q(x) \equiv b(x) \pmod{m(x)}$ es una solución de la congruencia.

Dos congruencias de la forma $a_1(x)p(x) \equiv b_1(x) \pmod{m_1(x)}$ y $a_2(x)p(x) \equiv b_2(x) \pmod{m_2(x)}$ son equivalentes si toda solución de la primera es solución de la segunda y viceversa.

La forma de resolver estas congruencias es análoga a la que seguíamos para resolverlas en \mathbb{Z} . Transformamos (si es posible) la congruencia $a(x)p(x) \equiv b(x) \pmod{m(x)}$ en otra equivalente de la forma $p(x) \equiv c(x) \pmod{n(x)}$, cuyas soluciones son

$$p(x) = c(x) + q(x)n(x) : \quad q(x) \in K[x]$$

Los resultados necesarios para resolver estas congruencias son:

1. Si $a_1(x) \equiv a_2(x) \pmod{m(x)}$ y $b_1(x) \equiv b_2(x) \pmod{m(x)}$ entonces las congruencias $a_1(x)p(x) \equiv b_1(x) \pmod{m(x)}$ y $a_2(x)p(x) \equiv b_2(x) \pmod{m(x)}$ son equivalentes.
2. Si $d(x)$ es un divisor común de $a(x)$, $b(x)$ y $m(x)$, las congruencias

$$a(x)p(x) \equiv b(x) \pmod{m(x)} \quad \frac{a(x)}{d(x)}p(x) \equiv \frac{b(x)}{d(x)} \pmod{\frac{m(x)}{d(x)}}$$

son equivalentes.

3. Si $\text{mcd}(m(x), c(x)) = 1$ entonces las congruencias

$$a(x)p(x) \equiv b(x) \pmod{m(x)} \quad c(x)a(x)p(x) \equiv c(x)b(x) \pmod{m(x)}$$

son equivalentes.

Proposición 3.5.1. Sea K un cuerpo, y $a(x), b(x), m(x) \in K[x]$ tales que $\text{gr}(m(x)) \geq 1$. Entonces

$$a(x)p(x) \equiv b(x) \pmod{m(x)}$$

tiene solución si, y sólo si, $\text{mcd}(a(x), m(x)) | b(x)$.

Para resolver congruencias de la forma $a(x)p(x) \equiv b(x) \pmod{m(x)}$ podemos proceder como sigue:

- ▮ Reducimos $a(x)$ y $b(x)$ módulo $m(x)$.
- ▮ Se comprueba si $\text{mcd}(a(x), m(x)) | b(x)$. Si la respuesta es negativa, entonces la congruencia no tiene solución. Si la respuesta es afirmativa, podemos dividir toda la congruencia por $\text{mcd}(a(x), m(x))$. Hemos transformado la congruencia en una de la forma $a(x)p(x) \equiv b(x) \pmod{m(x)}$, pero ahora se tiene que $\text{mcd}(a(x), m(x)) = 1$.
- ▮ Buscamos el inverso de $[a(x)]$ en $K[x]_{m(x)}$. Supongamos que es $[u(x)]$.
- ▮ Multiplicamos ambos miembros de la congruencia por $u(x)$. Obtenemos así una congruencia equivalente, y ésta adopta la forma $p(x) \equiv c(x) \pmod{m(x)}$.

Con esto ya hemos resuelto la congruencia. Las soluciones son $p(x) = c(x) + q(x)m(x) : q(x) \in K[x]$.

Ejemplo 3.5.1. Vamos a resolver en $\mathbb{Z}_{11}[x]$ la congruencia

$$(x^2 + 6x + 9)p(x) \equiv 3x^3 + 7x^2 + 9x + 2 \pmod{x^3 + 5x^2 + 10x + 3}$$

Reducimos módulo $x^3 + 5x^2 + 10x + 2$.

$$(x^2 + 6x + 9)p(x) \equiv 3x^2 + x + 4 \pmod{x^3 + 5x^2 + 10x + 3}.$$

Hallamos el máximo común divisor de $x^2 + 6x + 9$ y $x^3 + 5x^2 + 10x + 3$.

$p(x)$	$q(x)$	a
$x^3 + 5x^2 + 10x + 3$	$x^2 + 6x + 9$	
$x^2 + 6x + 9$	$7x + 1$	
$7x + 1$	3	
3	0	4
1		

Puesto que este máximo común divisor vale 1 hallamos el inverso de $x^2 + 6x + 9$ módulo $x^3 + 5x^2 + 10x + 3$.

a	$r(x)$	$c(x)$	$v(x)$
	$x^3 + 5x^2 + 10x + 3$		0
	$x^2 + 6x + 9$		1
	$7x + 1$	$x + 10$	$10x + 1$
	3	$8x + 6$	$8x^2 + 9x + 6$
4	0		
	1		$10x^2 + 3x + 2$

Multiplicamos por $10x^2 + 3x + 2$.

$$(10x^4 + 8x^3 + 6x + 7)p(x) \equiv 8x^4 + 8x^3 + 5x^2 + 3x + 8 \pmod{x^3 + 5x^2 + 10x + 3}.$$

Reducimos módulo $x^3 + 5x^2 + 10x + 3$.

$$p(x) \equiv 8x^2 + 2x + 5 \pmod{x^3 + 5x^2 + 10x + 3}.$$

Luego la solución es

$$p(x) = 8x^2 + 2x + 5 + c(x)(x^3 + 5x^2 + 10x + 3) : \quad c(x) \in \mathbb{Z}_{11}[x].$$

En lo referente a un sistema de congruencias se tiene también el teorema chino del resto.

Teorema 3.5.1. Sean $a_1(x), \dots, a_k(x) \in K[x]$ y sean $m_1(x), \dots, m_k(x) \in K[x]$ tales que $\text{mcd}(m_i(x), m_j(x)) = 1$. Entonces el sistema

$$\begin{aligned} p(x) &\equiv a_1(x) \pmod{m_1(x)} \\ p(x) &\equiv a_2(x) \pmod{m_2(x)} \\ &\dots\dots\dots \\ p(x) &\equiv a_k(x) \pmod{m_k(x)} \end{aligned}$$

tiene solución. Además, si $a(x)$ es una solución, el sistema es equivalente a la congruencia

$$p(x) \equiv a(x) \pmod{M(x)}$$

donde $M(x) = \prod_{i=1}^k m_i(x)$.

Sin embargo, a la hora de resolver sistemas de congruencias, procederemos a resolverlo progresivamente. Resolvemos la primera congruencia; introducimos esta solución en la segunda congruencia y la resolvemos; y así sucesivamente. De esta forma, no estamos sujetos a que se satisfagan las hipótesis del teorema chino. Veamos un ejemplo.

Ejemplo 3.5.2. Vamos a resolver el sistema de congruencias en $\mathbb{Z}_5[x]$.

$$\begin{aligned} p(x) &\equiv x + 2 \pmod{x^2 + 1} \\ (x + 1)p(x) &\equiv x^2 + 1 \pmod{x^3 + 2x^2 + 2} \\ x^2 p(x) &\equiv 3x + 2 \pmod{x^2 + x + 1} \end{aligned}$$

Resolvemos la primera congruencia:

$$p(x) = x + 2 + (x^2 + 1)q_1(x).$$

Introducimos esta solución en la segunda congruencia.

$$\begin{aligned} (x + 1)(x + 2 + (x^2 + 1)q_1(x)) &\equiv x^2 + 1 \pmod{x^3 + 2x^2 + 2}; \\ x^2 + 3x + 2 + (x^3 + x^2 + x + 1)q_1(x) &\equiv x^2 + 1 \pmod{x^3 + 2x^2 + 2}; \\ (x^3 + x^2 + x + 1)q_1(x) &\equiv 2x + 4 \pmod{x^3 + 2x^2 + 2}; \\ (4x^2 + x + 4)q_1(x) &\equiv 2x + 4 \pmod{x^3 + 2x^2 + 2}. \end{aligned}$$

A continuación calculamos el inverso de $4x^2 + x + 4$ módulo $x^3 + 2x^2 + 2$.

a	$r(x)$	$c(x)$	$v(x)$
	$x^3 + 2x^2 + 2$		0
	$4x^2 + x + 4$		1
	$2x + 4$	$4x + 2$	$x + 3$
	3	$2x + 4$	$3x^2 + 4$
2	0		
	1		$x^2 + 3$

Multiplicamos entonces por $x^2 + 3$.

$$\begin{aligned} q_1(x) &\equiv (x^2 + 3)(2x + 4) \pmod{x^3 + 2x^2 + 2}; \\ q_1(x) &\equiv 2x^3 + 4x^2 + x + 2 \pmod{x^3 + 2x^2 + 2}; \\ q_1(x) &\equiv x + 3 \pmod{x^3 + 2x^2 + 2}. \end{aligned}$$

Luego $q_1(x) = x + 3 + q_2(x)(x^3 + 2x^2 + 2)$ y por tanto $p(x) = x^3 + 3x^2 + 2x + q_2(x)(x^5 + 2x^4 + x^3 + 4x^2 + 2)$. Introducimos esta solución en la tercera congruencia, y operamos:

$$\begin{aligned} x^2(x^3 + 3x^2 + 2x) + x^2(x^5 + 2x^4 + x^3 + 4x^2 + 2)q_2(x) &\equiv 3x + 2 \pmod{x^2 + x + 1}; \\ (x^7 + 2x^6 + x^5 + 4x^4 + 2x^2)q_2(x) &\equiv 4x^5 + 2x^4 + 3x^3 + 3x + 2 \pmod{x^2 + x + 1}; \\ (2x + 4)q_2(x) &\equiv x + 1 \pmod{x^2 + x + 1}. \end{aligned}$$

Calculamos el inverso de $2x + 4$ módulo $x^2 + x + 1$, y resulta ser $4x + 1$. Multiplicamos entonces por este polinomio.

$$\begin{aligned} q_2(x) &\equiv (x + 1)(4x + 1) \pmod{x^2 + x + 1}; \\ q_2(x) &\equiv 4x^2 + 1 \pmod{x^2 + x + 1}; \\ q_2(x) &\equiv x + 2 \pmod{x^2 + x + 1}. \end{aligned}$$

Por tanto, se tiene que $q_2(x) = x + 2 + q(x)(x^2 + x + 1)$. Introducimos este valor en lo que ya teníamos para $p(x)$ y nos queda:

$$p(x) = x^3 + 3x^2 + 2x + [x + 2 + (x^2 + x + 1)q(x)](x^5 + 2x^4 + x^3 + 4x^2 + 2),$$

es decir:

$$p(x) = x^6 + 4x^5 + 2x^3 + x^2 + 4x + 1 + (x^7 + 3x^6 + 4x^5 + 2x^4 + x^2 + 2x + 2)q(x).$$

Un caso particularmente interesante es cuando queremos resolver un sistema de congruencias donde todos los módulos son polinomios mónicos (de la forma $x - a$). Para resolver este tipo de sistemas de congruencias es importante tener en cuenta que se verifica que

$$q(x) \equiv q(a) \pmod{x - a}$$

luego, para reducir un polinomio módulo $x - a$ basta con evaluar el polinomio en $x = a$.

Por otra parte, el inverso de $q(x)$ módulo $x - a$ es $q(a)^{-1}$ (este último calculado en K).

Por último, el problema de encontrar un polinomio $p(x)$ que satisfaga la congruencia $p(x) \equiv b \pmod{x - a}$ es equivalente al problema de encontrar un polinomio $p(x)$ que verifique que $p(a) = b$.

Nos planteamos entonces el siguiente problema:

Dados $a_0, a_1, \dots, a_m \in K$ todos distintos, y $b_0, b_1, \dots, b_m \in K$, encontrar un polinomio $p(x) \in K[x]$ tal que $p(a_i) = b_i$.

Este problema se conoce como *problema de interpolación* y un polinomio solución se dice que es un polinomio interpolador.

Para resolverlo, planteamos el siguiente sistema de congruencias:

$$\begin{aligned} p(x) &\equiv b_0 \pmod{x - a_0} \\ p(x) &\equiv b_1 \pmod{x - a_1} \\ &\dots\dots\dots \\ p(x) &\equiv b_m \pmod{x - a_m} \end{aligned}$$

Cada una de las soluciones de este sistema será un polinomio interpolador.

Puesto que $\text{mcd}(x - a_i, x - a_j) = 1$ para $i \neq j$ deducimos, a partir del teorema chino, que este sistema tiene solución. Además, la solución es única módulo $\prod_{i=0}^m (x - a_i)$. Puesto que este polinomio tiene grado $m + 1$, deducimos que existe siempre un polinomio de grado menor o igual que m que interpola $m + 1$ datos.

Ejemplo 3.5.3. *Vamos a encontrar un polinomio en $\mathbb{Z}_7[x]$ que satisfaga que $p(1) = 2$, $p(2) = 5$, $p(4) = 6$ y $p(5) = 5$.*

Para ello, planteamos el sistema de congruencias

$$\begin{aligned} p(x) &\equiv 2 \pmod{x + 6} \\ p(x) &\equiv 5 \pmod{x + 5} \\ p(x) &\equiv 6 \pmod{x + 3} \\ p(x) &\equiv 5 \pmod{x + 2} \end{aligned}$$

y procedemos a resolverlo como siempre:

Hallamos la solución de la primera congruencia

$$p(x) = 2 + (x + 6)q_1(x).$$

Introducimos esta solución en la segunda congruencia y operamos.

$$\begin{aligned} 2 + (x + 6)q_1(x) &\equiv 5 \pmod{x + 5}; \\ (x + 6)q_1(x) &\equiv 3 \pmod{x + 5}; \end{aligned}$$

$$q_1(x) \equiv 3(\text{mód } x + 5);$$

$$q_1(x) = 3 + q_2(x)(x + 5).$$

Luego resulta que $p(x) = 2 + (x + 6)[3 + q_2(x)(x + 5)] = 3x + 6 + (x + 6)(x + 5)q_2(x)$.

Continuamos introduciendo esta solución en la tercera congruencia.

$$3x + 6 + (x + 6)(x + 5)q_2(x) \equiv 6(\text{mód } x + 3);$$

$$(x + 6)(x + 5)q_2(x) \equiv 4x(\text{mód } x + 3);$$

$$6q_2(x) \equiv 2(\text{mód } x + 3);$$

$$q_2(x) \equiv 5(\text{mód } x + 3);$$

$$q_2(x) = 5 + q_3(x)(x + 3).$$

Por tanto, $p(x) = 3x + 6 + (x + 6)(x + 5)[5 + q_3(x)(x + 3)] = 5x^2 + 2x + 2 + (x + 6)(x + 5)(x + 3)q_3(x)$.

$$5x^2 + 2x + 2 + (x + 6)(x + 5)(x + 3)q_3(x) \equiv 5(\text{mód } x + 2);$$

$$(x + 6)(x + 5)(x + 3)q_3(x) \equiv 2x^2 + 5x + 3(\text{mód } x + 2);$$

$$5q_3(x) \equiv 1(\text{mód } x + 2);$$

$$q_3(x) \equiv 3(\text{mód } x + 2);$$

$$q_3(x) = 3 + q(x)(x + 2).$$

Nos queda entonces que $p(x) = 5x^2 + 2x + 2 + (x + 6)(x + 5)(x + 3)[3 + (x + 2)q(x)]$, es decir,

$$p(x) = 3x^3 + 5x^2 + 2x + 6 + (x + 6)(x + 5)(x + 3)(x + 2)q(x),$$

luego una solución es $p(x) = 3x^3 + 5x^2 + 2x + 6$.

Basándonos en esta idea podemos diseñar un algoritmo que calcule un polinomio que interpole unos datos dados. Denominaremos a este algoritmo INTERPOLA

Algoritmo INTERPOLA($m, a_0, b_0, a_1, b_1, \dots, a_m, b_m$)

Entrada:

$$m \in \mathbb{N}$$

$$a_0, b_0, a_1, b_1, \dots, a_m, b_m \in K$$

Salida: $p(x) \in K[x]$. $p(a_i) = b_i$ y $\text{gr}(p(x)) \leq n$

$$p(x) := b_0$$

$$q(x) := x - a_0$$

Desde $i = 1$ hasta m

$$p(x) := p(x) + q(a_i)^{-1}(b_i - p(a_i)) \cdot q(x)$$

$$q(x) := q(x) \cdot (x - a_i)$$

Devuelve $p(x)$

Fin

Veamos como resolver el ejemplo anterior haciendo uso de este algoritmo.

i	a_i	b_i	$q(a_i)$	$q(a_i)^{-1}$	$p(a_i)$	$b_i - p(a_i)$	$p(x)$	$q(x)$
							2	$x + 6$
1	2	5	1	1	2	3	$3x + 6$	$x^2 + 4x + 2$
2	4	6	6	6	4	2	$5x^2 + 2x + 2$	$x^3 + 6$
3	5	5	5	3	4	1	$3x^3 + 5x^2 + 2x + 6$	$x^4 + 2x^3 + 6x + 5$

Luego el polinomio interpolador es $p(x) = 3x^3 + 5x^2 + 2x + 6$. Todos los polinomios que satisfacen las condiciones dadas adoptan la forma:

$$p(x) = 3x^3 + 5x^2 + 2x + 6 + c(x)(x^4 + 2x^3 + 6x + 5) : \quad c(x) \in \mathbb{Z}_7[x]$$

Vamos a comprobar que el polinomio $p(x)$ satisface las condiciones requeridas. Para ello, vamos a evaluarlo en $x = 1$, $x = 2$, $x = 4$ y $x = 5$.

1	3	5	2	6	2	3	5	2	6	4	3	5	2	6	5	3	5	2	6
		3	1	3			6	1	6			5	5	0			1	2	6
	3	1	3	2		3	4	3	5		3	3	0	6		3	6	4	5

$$p(1) = 2$$

$$p(2) = 5$$

$$p(4) = 6$$

$$p(5) = 5$$

Si nos fijamos en el algoritmo, vemos que lo que hacemos es expresar el polinomio interpolador como

$$p(x) = c_0 + c_1(x - a_0) + c_2(x - a_0)(x - a_1) + \cdots + c_n(x - a_0)(x - a_1) \cdots (x - a_{n-1})$$

Y el algoritmo nos calcula los coeficientes c_i . De hecho, se tiene que $c_i = q(a_i)^{-1}(b_i - p(a_i))$.

Estos coeficientes pueden calcularse también haciendo uso de las diferencias divididas. Vemos en que consiste.

Definición 55. Sea K un cuerpo, y $f : K \rightarrow K$ una aplicación. Sean $a_0, a_1, \dots, a_n \in K$ todos distintos. Se definen las diferencias divididas $f[a_i, a_{i+1}, \dots, a_{i+k}]$ como sigue:

$$f[a_i] = f(a_i)$$

$$f[a_i, a_{i+1}, \dots, a_{i+k}] = \frac{f[a_{i+1}, \dots, a_{i+k}] - f[a_i, \dots, a_{i+k-1}]}{a_{i+k} - a_i}$$

donde hemos usado la notación $\frac{a}{b}$ para representar $a \cdot b^{-1}$.

Ejemplo 3.5.4.

Sea $K = \mathbb{Z}_5$, sean $a_0 = 1$, $a_1 = 2$ y $a_2 = 4$, y sea $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ la aplicación dada por $f(x) = x^2 + 2x$. Entonces:

$$f[a_0] = f(1) = 3$$

$$f[a_1] = f(2) = 3 \quad f[a_0, a_1] = \frac{f[a_1] - f[a_0]}{a_1 - a_0} = \frac{3-3}{2-1} = 0$$

$$f[a_2] = f(4) = 4 \quad f[a_1, a_2] = \frac{f[a_2] - f[a_1]}{a_2 - a_1} = \frac{4-3}{4-2} = 1 \cdot 3 = 3 \quad f[a_0, a_1, a_2] = \frac{f[a_1, a_2] - f[a_0, a_1]}{a_2 - a_0} = \frac{3-0}{4-1} = 1$$

El interés de las diferencias divididas viene dado en el siguiente teorema.

Teorema 3.5.2. Sea K un cuerpo, $a_0, a_1, \dots, a_n \in K$ distintos, y $b_0, b_1, \dots, b_n \in K$. Sea $p(x)$ el polinomio interpolador para estos datos, es decir, $p(x) \in K[x]$, $\text{gr}(p(x)) \leq n$ y $p(a_i) = b_i$. Entonces:

$$p(x) = p[a_0] + p[a_0, a_1](x - a_0) + p[a_0, a_1, a_2](x - a_0)(x - a_1) + \cdots + p[a_0, a_1, \dots, a_n](x - a_0)(x - a_1) \cdots (x - a_{n-1})$$

o en notación más compacta

$$p(x) = \sum_{i=0}^n p[a_0, \dots, a_i](x - a_0) \cdots (x - a_{i-1})$$

Ejemplo 3.5.5.

Vamos a calcular $p(x) \in \mathbb{Z}_5[x]$ que interpola a los datos $p(1) = 3$, $p(2) = 3$, $p(4) = 4$. Por el ejemplo 3.5.4 sabemos que ese polinomio es $p(x) = x^2 + 2x$.

Según el teorema que acabamos de ver, se tiene que

$$p(x) = p[1] + p[1, 2](x - 1) + p[1, 2, 4](x - 1)(x - 2) = 3 + 0(x - 1) + 1(x - 1)(x - 2) = 3 + x^2 - 3x + 2 = x^2 + 2x$$

El siguiente algoritmo nos calcula el polinomio interpolador haciendo uso de las diferencias divididas.

Algoritmo NEWTON($m, a_0, b_0, a_1, b_1, \dots, a_m, b_m$)

Entrada:

$$m \in \mathbb{N}$$

$$a_0, b_0, a_1, b_1, \dots, a_m, b_m \in K$$

Salida: $p(x) \in K[x]$. $p(a_i) = b_i$ y $\text{gr}(p(x)) \leq m$

$$p(x) := b_0$$

$$q(x) := (x - a_0)$$

Desde $i = 1$ hasta m

Desde $j = m$ hasta i paso: (-1)

$$b_j := \frac{b_j - b_{j-1}}{a_j - a_{j-1}}$$

$$p(x) := p(x) + b_i \cdot q(x)$$

$$q(x) := q(x) \cdot (x - a_i)$$

Devuelve $p(x)$

Fin

Ejemplo 3.5.6.

Vamos a calcular $p(x) \in \mathbb{Z}_7[x]$ tal que $p(1) = 2$, $p(2) = 5$, $p(4) = 6$ y $p(5) = 5$. Es decir, el mismo polinomio que obtuvimos en el ejemplo 3.5.3.

Los cálculos que vayamos haciendo los vamos a representar en una tabla.

Comenzamos inicializando las variables.

	$i = 0$					
	a_j	b_j			$p(x)$	$q(x)$
$j = 0$	1	2			2	$x + 6$
$j = 1$	2	5				
$j = 2$	4	6				
$j = 3$	5	5				

Y ahora entramos en el bucle, con $i = 1$. Calculamos

$$b_3 = \frac{b_3 - b_2}{a_3 - a_2} = \frac{5 - 6}{5 - 4} = (-1) \cdot 1^{-1} = 6.$$

$$b_2 = \frac{b_2 - b_1}{a_2 - a_1} = \frac{6 - 5}{4 - 2} = 1 \cdot 2^{-1} = 4.$$

$$b_1 = \frac{b_1 - b_0}{a_1 - a_0} = \frac{5 - 2}{2 - 1} = 3 \cdot 1^{-1} = 3.$$

$$p(x) = p(x) + b_1 \cdot q(x) = 2 + 3(x + 6) = 2 + 3x + 18 = 3x + 6.$$

$$q(x) = q(x)(x - a_1) = (x + 6)(x - 2) = (x + 6)(x + 5) = x^2 + 4x + 2.$$

	$i = 0$		$i = 1$			
	a_j	b_j	b_j		$p(x)$	$q(x)$
$j = 0$	1	2			2	$x + 6$
$j = 1$	2	5	3		$3x + 6$	$x^2 + 4x + 2$
$j = 2$	4	6	4			
$j = 3$	5	5	6			

Continuamos en el bucle, ahora para $i = 2$.

$$b_3 = \frac{b_3 - b_2}{a_3 - a_2} = \frac{6 - 4}{5 - 2} = 2 \cdot 3^{-1} = 3.$$

$$b_2 = \frac{b_2 - b_1}{a_2 - a_0} = \frac{4 - 3}{4 - 1} = 1 \cdot 3^{-1} = 5.$$

$$p(x) = p(x) + b_2 q(x) = 3x + 6 + 5(x^2 + 4x + 2) = 5x^2 + 23x + 16 = 5x^2 + 2x + 2.$$

$$q(x) = q(x)(x - a_2) = (x^2 + 4x + 2)(x - 4) = (x^2 + 4x + 2)(x + 3) = x^3 + 6.$$

	$i = 0$		$i = 1$	$i = 2$		
	a_j	b_j	b_j	b_j	$p(x)$	$q(x)$
$j = 0$	1	2			2	$x + 6$
$j = 1$	2	5	3		$3x + 6$	$x^2 + 4x + 2$
$j = 2$	4	6	4	5	$5x^2 + 2x + 2$	$x^3 + 6$
$j = 3$	5	5	6	3		

Por último, entramos en el bucle, con $i = 3$.

$$b_3 = \frac{b_3 - b_2}{a_3 - a_0} = \frac{3 - 5}{5 - 1} = (-2) \cdot 4^{-1} = 5 \cdot 2 = 3.$$

		$i = 0$	$i = 1$	$i = 2$	$i = 3$		
	a_j	b_j	b_j	b_j	b_j	$p(x)$	$q(x)$
$j = 0$	1	2				2	$x + 6$
$j = 1$	2	5	3			$3x + 6$	$x^2 + 4x + 2$
$j = 2$	4	6	4	5		$5x^2 + 2x + 2$	$x^3 + 6$
$j = 3$	5	5	6	3	3	$3x^3 + 5x^2 + 2x + 6$	$x^4 + 2x^3 + 6x + 5$

Y tenemos al final el polinomio interpolador.

Observaciones:

1. Tal y como hemos descrito el algoritmo, al calcular el valor de una diferencia dividida borra uno que existía previamente, de tal forma que al final sólo quedarían guardados aquellos valores que se utilizan para calcular el polinomio de Newton. En el ejemplo que hemos hecho, tendríamos al final $b_0 = 2$, $b_1 = 3$, $b_2 = 5$ y $b_3 = 3$. Si quisiéramos almacenarlos todos deberíamos crear una matriz b_{ij} para las diferencias divididas.

En la tabla, no obstante, hemos conservado todos estos valores.

2. Si hemos calculado un polinomio por este método, y nos añaden un dato nuevo, los cálculos realizados nos sirven para calcular el nuevo polinomio. Bastaría con añadir una nueva fila al final, y calcular las correspondientes diferencias divididas.

Por ejemplo, supongamos que además de las condiciones expresadas anteriormente ($p(1) = 2$, $p(2) = 5$, $p(4) = 6$ y $p(5) = 5$) nos dicen que el polinomio debe verificar que $p(3) = 1$.

Tendríamos entonces $a_4 = 3$ y $b_4 = 1$

		$i = 0$	$i = 1$	$i = 2$	$i = 3$		
	a_j	b_j	b_j	b_j	b_j	$p(x)$	$q(x)$
$j = 0$	1	2				2	$x + 6$
$j = 1$	2	5	3			$3x + 6$	$x^2 + 4x + 2$
$j = 2$	4	6	4	5		$5x^2 + 2x + 2$	$x^3 + 6$
$j = 3$	5	5	6	3	3	$3x^3 + 5x^2 + 2x + 6$	$x^4 + 2x^3 + 6x + 5$
$j = 4$	3	1					

Y ahora completariamos la última fila:

$$\text{Para } i = 1, b_4 = \frac{b_4 - b_3}{a_4 - a_3} = \frac{1 - 5}{3 - 5} = (-4) \cdot (-2)^{-1} = 3 \cdot 5^{-1} = 2.$$

$$\text{Para } i = 2, b_4 = \frac{b_4 - b_3}{a_4 - a_2} = \frac{2 - 6}{3 - 4} = (-4) \cdot (-1)^{-1} = 4 \cdot 1^{-1} = 4.$$

$$\text{Para } i = 3, b_4 = \frac{b_4 - b_3}{a_4 - a_1} = \frac{4 - 3}{3 - 2} = 1 \cdot 1^{-1} = 1.$$

$$\text{Para } i = 4, b_4 = \frac{b_4 - b_3}{a_4 - a_0} = \frac{1 - 3}{3 - 1} = (-2) \cdot 2^{-1} = -1 = 6.$$

Y una vez calculado esto, tendríamos:

$$p(x) = p(x) + b_4 q(x) = 3x^3 + 5x^2 + 2x + 6 + 6(x^4 + 2x^3 + 6x + 5) = 6x^4 + x^3 + 5x^2 + 3x + 1.$$

$$q(x) = q(x)(x - a_4) = (x^4 + 2x^3 + 6x + 5)(x - 3) = (x^4 + 2x^3 + 6x + 5)(x + 4) = x^5 + 6x^4 + x^3 + 6x^2 + x + 6.$$

		$i = 0$	$i = 1$	$i = 2$	$i = 3$	$i = 4$		
	a_j	b_j	b_j	b_j	b_j	b_j	$p(x)$	$q(x)$
$j = 0$	1	2					2	$x + 6$
$j = 1$	2	5	3				$3x + 6$	$x^2 + 4x + 2$
$j = 2$	4	6	4	5			$5x^2 + 2x + 2$	$x^3 + 6$
$j = 3$	5	5	6	3	3		$3x^3 + 5x^2 + 2x + 6$	$x^4 + 2x^3 + 6x + 5$
$j = 4$	3	1	2	4	1	6	$6x^4 + x^3 + 5x^2 + 3x + 1$	$x^5 + 6x^4 + x^3 + 6x^2 + x + 6$